

シティサプライヤー要件

オーナー

シティプロキュアメント&リスク責任者

発行日

2015 年 1 月

改訂日

2026 年 9 月

バージョン

9

目次

1	概要	4
2	雇用機会均等	6
3	贈収賄・汚職防止（AB&C）	7
4	贈答品と接待	8
5	サプライヤーの取り組みとサプライヤー原則	9
6	現代奴隷の禁止	9
7	サプライヤー人員	12
8	不正管理	13
9	メディアへの対応と公式会見	16
10	電子的な文書によるコミュニケーション	16
11	政治活動と献金	17
12	マネーロンダリング対策（「AML」）	18
13	記録管理	20
14	ビジネスのエンタープライズレジリエンス/継続性	22
15	身元調査のグローバル基準	30
16	経費	33
17	情報セキュリティ（IS）	34
18	安全な職場に関するガイドライン	85
19	人工知能/機械学習（生成 AI/エージェント型 AI を含む）	86
20	顧客からの苦情	88
21	個人での売買および投資に関するポリシー	89
22	請求と請求書作成基準	89

23	職場離脱ポリシー	90
付録 - 定義		92

1 概要

1.1. 一般的な要件

本「シティサプライヤー要件」（以下「**要件**」）は、サプライヤーがシティと取引を行う上で満たすべき義務の一部を詳述するものです。特定の要件はすべてのサプライヤーに適用されますが、その他の要件が特定のサプライヤーに適用されるかどうかはサプライヤーがシティに提供する製品およびサービスの種類によって異なります（後者は下記第 1.2 項に要約され、そこに記載される各条項の冒頭に示されています）。英語原文において大文字で表記された用語は、添付の付録を含め、本書に記載された意味を有するものとします。ただし、本書にそのような意味が記載されていない場合、以下に定義するとおり、本書に記載された意味を有するものとします。

本要件は、サプライヤーとシティとの契約（作業指示書、ライセンススケジュールなどの取引文書を含むがこれに限らない）（以下「**契約**」）に基づく契約上の義務であり、契約に定める義務、適用法（以下に定義します）に基づく義務、シティからサプライヤーへの本義務に関する通知（以下「**通知**」）、またはシティの事業もしくは部門により実施される追加のより詳細な義務に加え適用されるものです。前述の要件と本要件の間に矛盾がある場合は、より制限的な義務および要件が適用されるものとします。サプライヤーは、本要件の変更、適用除外の要求、または本要件や適用法との抵触の認識など、本要件に関する質問について、積極的な役割を果たし、シティの主要な業務担当者（またはその被指名人）に相談するものとします。

サプライヤーは、適用法を遵守するシティの義務に関連して、シティがサプライヤーサービスまたは従業員に関連して必要とするデータについて、シティがサプライヤーに対してできる合理的な要求を速やかに遵守するものとします。サプライヤーがこれらの義務を遵守しなかった場合、本契約条件への重大な違反とみなされます。

これらの要件、またはサプライヤーが取引するシティのビジネスが指定する追加的要件に従わない場合、サプライヤーとシティとの契約が終了する場合があります。さらに、本要件に違反した場合、適用法にも違反する可能性があり、シティ（または第三者）に民事上の損害賠償を負わせたり、サプライヤーに刑事罰を科したりする可能性があります。サプライヤーは、シティの書面による同意がない限り、本要件のいずれかの条項を遵守する義務の代用として、独自のポリシーの遵守を使用することはできません。

1.2. 一部のサプライヤーに適用される要件

次の表は、指定された適用基準を満たす特定のサプライヤーに適用される特定の要件を示しています。以下に記載されていない項は、すべてのサプライヤーに適用されます。

項番号	項名	適用対象
2	雇用機会均等/差別是正措置	適用対象：米国連邦政府とのシティ契約の履行に必要な契約および発注書。当該契約または発注書が連邦政府の下請契約または発注書に該当するか不明確な場合は、条項の冒頭または末尾に、状況に応じて「該当する場合」と記載してください。
12	マネーロンダリング対策	適用対象：サプライヤーが特定の顧客関連サービス（オンボーディング、顧客アカウントや取引のスクリーニング）を行う際、または前述の活動に関連したデータ/メトリクスの送信時、 <u>および/または</u> サプライヤーが現金または金融商品（オンラインデポジット、宅配便、現金輸送車、または金庫サービスなど）関連の仲介を務める場合
13	記録管理	適用対象：シティ情報のアクセス/処理/保管を行うサプライヤー
14	業務継続	適用対象：シティが使用するサービスまたはホストテクノロジーのインフラストラクチャ/アプリケーションを提供するサプライヤー。適用対象およびビジネスの持続性（Cobb）要件をサプライヤーに通知することは、シティビジネス活動担当責任者（BAO）の責任
15	身元調査のグローバル基準	適用対象：シティにサービスを提供するサプライヤー
16	経費	適用対象：事業活動費の払い戻しを請求する契約上の資格があるサプライヤー
17	情報セキュリティ（IS）	適用対象：シティの情報のアクセス/処理/管理/保管を行う業務委託先を含むサプライヤー <u>および/または</u> インターネットに接続するシティブランドアプリケーションをホスティングする責任を担うサプライヤー、 <u>および/または</u> シティのネットワークリソースに接続するサプライヤー、 <u>および/または</u> シティ施設に同伴者なしでアクセスする必要があるサプライヤー
18	安全な職場に関するガイドライン	

項番号	項名	適用対象
19	人工知能/機械学習（生成 AI/エージェント型 AI を含む）	適用対象：提供する商品/サービスの一部にシティが定義する人工知能/機械学習(AI/ML)を活用しているサプライヤー
20	個人での売買および投資に関するポリシー	適用対象：シティでの職務の一環として MNPI に定期的にアクセスする必要があるサプライヤー
23	職場離脱ポリシー	本ポリシーは、（用語集で定義される）機密性の高い職務に就く非従業員（「労働者」）（「機密性の高い」労働者）、ならびに機密性の高い職務に就く従業員の直属の上司および監督者（「マネージャー」）、ならびに機密性の高い非従業員のシティの業務上の連絡先に適用されます。

2 雇用機会均等

2.1 雇用機会均等

シティでは、人種、肌の色、宗教、性別、性的指向、性同一性（ジェンダー・アイデンティティ）、出身国、国籍、移民ステータス、年齢、配偶者の有無、遺伝子情報、障害、保護の対象となる退役軍人ステータス、または法律により保護されているその他の特徴にかかわらず、すべての適格者について雇用機会均等化を確実にするためのポリシーを開発しました。

サプライヤーは、適用されるすべての差別禁止の法律および規制（シティがサプライヤーに遵守するよう書面で通知する法律または規制を含むがこれに限定されない）の要件を遵守し、また彼らの人員に遵守させるものとします。

サプライヤーは、シティの米国雇用機会均等ポリシーステートメント（www.citigroup.com/global/eeo-aa-policy）を精査し、これに従って適切な措置取るものとします。

2.2 政府契約

連邦政府とのシティ契約を実行するために必要な契約および発注には、以下の条項を逐語的に含める必要があります。（連邦政府の下請け/発注であるかどうか分からない場合には、セクションの冒頭に「該当する場合」を含めてください）。

【該当する場合、】サプライヤーは、適用されるすべての連邦差別禁止法を遵守し、適用される連邦差別禁止法に違反したプログラムを実施していないことを証明するものとします。

2.3 政府契約の付録

連邦政府とシティとの契約の履行に必要な契約および発注には、業務委託先または発注書の付録に以下の通知を含める必要があります。（連邦政府の下請け/発注であるかどうかかわからない場合には、以下の通知の最後に「該当する場合」を含めてください）。

連邦政府業務委託先として、シティグループはここに、保護されている退役軍人および障害のある個人に代わって、当社の雇用機会均等を書面で通知する、署名のない業務委託先またはベンダーを提供します。シティグループは、リハビリテーション法第503条およびベトナム戦争参加兵士保護法、ならびにそれぞれ 41 C.F.R. § 60-741 および 41 C.F.R. § 60-300 に基づく適用規制を完全に遵守しています。当社の Equal Employment Opportunity Policy ステートメントは、www.citigroup.com/global/eeo-aa-policy に記載されています。当社の EEO（雇用機会均等）ポリシーステートメントに関する質問は、ポリシーステートメントにある連絡先に問い合わせできます。

【該当する場合】、当社のポリシーステートメントおよび規制に沿った適切な行動を取ることを要求します。

3 贈収賄・汚職防止（AB&C）

シティは、適用される AB&C 法に準拠するために合理的に設計されたポリシー、手順、および内部統制を策定しており、贈収賄や円滑化（便宜）のための支払いを固く禁じています。（ビジネスイントロデューサーを含む）サプライヤー、その従業員、またはシティに代わって行動するすべての個人は、最高水準の倫理基準に従って、またシティが業務を行う国の米国海外腐敗行為防止法（FCPA）、英国の贈収賄禁止法（UKBA）、各改訂版、およびその他適用されるすべての現地 AB&C 法を遵守して活動するものとします。

サプライヤー、またはシティを代表して活動するその人員のいずれも、またはサプライヤーのシティとの契約または関係に関連して、(i)いかなる者に対して、支払い、利

益、利点、またはその他の価値のあるものを供与、授与、許可、または提案すること、(ii)いかなる者から支払、利益、利点、またはその他の価値のあるものを受領または受領することをいずれの場合も(i)-(ii) FCPA、UKBA、またはその他の AB&C 法に違反することを行わないものとします。サプライヤーとその従業員は、本セクションを含む要件に従い、シティに代わって、またはサプライヤーのシティとの契約または関係に関連して活動および取引を行う必要があります。サプライヤーとその従業員は、AB&C コンプライアンスプログラム、および AB&C のすべての法律を確実に遵守するために設計・適用されたポリシーと手順も維持する必要があります。

シティの AB&C プログラムの概要については、[Citigroup's Investor Relations](#)（「シティポリシー」から「AB&C プログラム」を選択）を参照してください。

4 贈答品と接待

サプライヤーもその人員も、シティの従業員に贈答品や有価物（接待も含む）を提供できません。これを行うと利益相反の状況を生んだり、対価とみなされたり、利益相反と見なされたり、従業員の誠実さや判断に疑いを持たれたり、従業員の意思決定に不適切な影響を与えたり、従業員の義務に反する行動の要因となったり、適用法への違反となったりする可能性があります。上記に制限されることなく、従業員は G&E 基準の禁止されている贈答品と接待セクションを遵守する必要があります。サプライヤーとその従業員は、合計で 1 人当たり年間 300 米ドルを超える現金以外のビジネス上の贈答品をシティの従業員に提供してはなりません。

サプライヤーがビジネス接待（食事、スポーツ、文化イベントなど）をシティ従業員に提供する場合、サプライヤーも当該イベントに出席することが必要です。またこうした接待は適切で習慣的かつ妥当なものでなくてはならず、贅沢であったり、過度に頻繁であったりするものであってはなりません。さらに、サプライヤーがイベントに出席していない場合、接待は業務上の贈答品とみなされ、シティの贈答品および接待基準で適用される報告基準の対象となります。サプライヤーは、シティを代表して、またはシティを装って、サプライヤー自身の費用またはシティ従業員の費用で、直接的または間接的に、あるいは他の人に同じことをするように促すなど、価値ある物品

を提供することはできません。そうすることは、汚職行為、不適切な行為、または適用法違反であると合理的に見なされる、またはそのように見なされます。

5 サプライヤーの取り組みとサプライヤー原則

<https://www.citigroup.com/citi/suppliers/> シティは、さまざまな取り組みを通じてサプライヤーと連携するとともに、当社が事業を展開する地域社会における潜在的なサプライヤーに対し、シティの調達プログラムに関する認知度向上を図っています。さらに、これらの取り組みは、有望なサプライヤー、特に新たなビジネス課題に対処するために革新的なソリューションを推進するサプライヤーを特定することを目的としています。シティがサプライヤーに期待するその他の情報は、以下の [Doing Business with Citi](#) サイトに記載されています。

[Citi Statement of Supplier Principles](#)
[Citi Sustainable Progress Strategy](#)

6 現代奴隷の禁止

シティは、現代の奴隷制度および人身売買が組織内またはそのサプライチェーン内で行われえるというリスクを特定し、防止することを目的とした慣習の維持に尽力しています。シティのサプライヤーは、以下に定める要件を遵守し、自らの業務およびサプライチェーンにおける現代奴隷および人身売買のリスクを特定し、防止することを目的とした効果的な全社的ポリシー、手順および/または実践を策定するものとします。サプライヤーは、シティの要請に応じて、求められるあらゆる付加的な情報を含め、シティの企業責任質問票に記入する必要があります。これは、特にリスクの高い分野や地域のサプライヤーのリスクエクスポージャーと潜在的な軽減策をシティが評価できるようにするものです。サプライヤーの業務委託先も、同様のプロセスに従うことが期待されています。

6.1 児童労働の禁止

サプライヤーは、児童労働を使用してはなりません。「児童」という用語は、適用される法令で定められた最低就業年齢未満の者を指し、そのような法令がない場合は、15 歳未満の者、または義務教育修了年齢未満の者のうち、いずれか年長の者を意味します。児童労働の使用に関して最優先される禁止法を条件として、18 歳未満の労働者が雇用される場合、児童の労働または労働条件の直接的または間接的結果として、児

童に身体的、精神的またはその他の危害が及ばないように、児童が遂行する義務、および労働条件に関して細心の注意を払うものとします。

6.2 自由意思に基づく雇用

サプライヤーは、労働者が、強制労働、精神的もしくは身体的強要、債務による拘束や年季奉公労働を強いられず、非自主的な囚人労働、奴隷、人身売買、または強制的な残業を含むあらゆる形態の強制的労働の対象とならないようにするものとします。すべての労働は自主的に行われなければなりません。本要件に基づくサプライヤーの義務には、以下を確保することが含まれますが、これらに限定されるものではありません。

1. **契約、賃金、労働時間**：労働者は、雇用または契約の条件を、労働者が理解しやすく、権利と義務を明確に記載した書面を用意されなければならないものとします。この書面には、賃金、残業手当、支払い期間、労働時間、ならびに休憩時間および休日に関する権利についての透明性のある条件（ただしこれらに限定されない）が記載されるものとします。かかる書面による条件は、勤務開始に先立って労働者に提供されるものとし、雇用主によって履行され、業界基準、ならびに業務が実施される場所の適用法および労働協約の最低要件を満たすものとします。
2. **仕事を自由に辞める権利**：労働者は、適用法および労働協約に基づいた合理的な通知期間後（必要に応じて）、不当な罰則を科されることなく、その雇用を自由に終了する権利を保有するものとします。
3. **非人道的な扱い**：労働者、その家族、および労働者と密接な関係にある者は体罰、身体的、心理的もしくは性的な暴力もしくは強要、暴言、ハラスメントまたは脅迫を含むがこれらに限定されない、苛酷または非人道的な扱いを受けないものとします。移民労働者、その家族、および労働者と密接な関係にある者は、その国籍によって雇用条件や労働条件における差別を受けないものとします。
4. **賃金、福利厚生、労働時間**：報酬は、最低賃金、残業手当、および法的に義務付けられている手当など、賃金に関するすべての適用法に準拠していなけ

ればなりません。従業員には、全額を期日通りに支払い、透明性のある給与明細書を交付しなければなりません。懲戒措置として、賃金や福利厚生から懲罰的な控除を行ったり、その支払いを差し控えたりしてはなりません。週単位の労働時間は、現地の法律で定められた最大労働時間を超えてはならず、時間外労働は本人の自発的な意志に基づくものでなければならず、また、法的な制限の範囲内で行われなければなりません。さらに、時間外労働を拒否したことを理由に不利益な扱いを受けてはなりません。

5. **身分証明書の没収禁止：**労働者は、雇用の条件として身分証明書、再入国許可証、パスポートなどの公的文書、またはその他貴重品を没収もしくは保留されないものとし、財産の差し押さえは、直接的または間接的に労働者の自由を制限したり、職場での奴隷労働を作り出したりするために使用されないものとしします。
6. **就職斡旋料または借金による拘束の禁止：**労働者の採用に関連する手数料または費用（就労ビザ関連の手数料、旅費および書類作成費用を含むがこれらに限定されない）は、直接的または間接的に関わらず、労働者に課されることはありません。同様に、労働者は、保証金を含め、職場での奴隷労働を意図する、もしくは効果を有する支払い（保証金を含む）を要求されたり、労働を通じて借金を返済するよう要求されたりしてはならないものとしします。採用手続き中または雇用期間中に従業員に手数料や費用が請求された場合、サプライヤーは、当該費用が速やかに払い戻されるよう、合理的な措置を講じなければなりません。人材紹介会社などの第三者を通じて手配される労働者の採用が必要となる場合は、信頼できる人材派遣会社のみを利用するものとしします。労働者を直接雇用する場合は、信頼できる人材紹介会社のみを使用するものとしします。労働者が負担する紹介手数料の禁止は、すべての採用担当者、人材紹介会社、および業務委託先人材紹介会社に適用されます。サプライヤーは、コンプライアンスを確実に遵守するための管理措置を講じなければなりません。**移動の自由：**労働者は、不当な制限を受けることなく自由に移動することができ、職場や雇用主が管理するその他の場所（寮など）に物理的に拘禁されないものとしします。実施される業務の場所または性質に

よって必要となる場合を除き、雇用主が管理する施設に宿泊する要件が労働者に課されないものとします。

- 7. 報復のない苦情申し立て：**労働者はそれぞれの雇用主に対し、雇用主による労働者の扱いに関する苦情を自由に申し立てることができ、労働者は苦情を申し立てたことに対して不利益、報復または迫害を受けないものとします。

7 サプライヤー人員

7.1 サプライヤーの人材育成、配置、再配置、管理

サプライヤーは、あらゆる契約に沿った最も効果的な方法で本サービスを実施するために、適切な訓練、教育、経験、および技能を有する十分な人数の従業員を使用し、要求に応じてかかる従業員の資格を証明するものとします。人員がプロジェクトに配属された後、サプライヤーは、シティの事前の書面による同意なしに、本プロジェクトに従事する能力を低下させるような他の案件への再配属または活用を行うことなく、通常、再配属の必要性により生じる混乱を最小限に抑える方法で、プロジェクトに人員を配属するものとします。サプライヤーは、自社の人員がシティの従業員または代理人であると自称したり、いかなる目的においてもシティの従業員として扱われることを求めたりしないことを確認します。これには、シティが提供する福利厚生、就業不能給付金、社会保障税または給付、連邦失業税、州失業保険給付または連邦所得税の源泉徴収に対する受給権の請求が含まれるものとします。サプライヤーは、その人員に関するすべての雇用主関連の責任（必要なすべての保険の維持、該当するすべての税務申告、およびサプライヤーの独立業務委託先としての地位と整合する方法による必要なすべての納税と預金を含むがこれに限定されない）を単独で負うものとします。

7.2 サプライヤーの人員の交代

サプライヤーは、サプライヤーがプロジェクトに配属した人員を、差別的でない理由でシティが容認できないとサプライヤーに通知した場合、その人員を排除し、交代させるものとします。サプライヤーはさらに、プロジェクトに配属された人員が適時かつ専門的な方法でサービスを提供できない、または提供する意志がない場合、直ちに当該人員を解任し交代させ、シティに対するサービスの提供（またはサービスの提供もしくは監督に関する一切の責任）から排除することに同意するものとします。

7.3 サプライヤーの人員ポリシー

サプライヤーは、自然人でありシティにオンサイトサービスを提供するために任命された人員の適格性認定に関する包括的なポリシーおよび手続きを維持し、効果的に管理すること、およびそれらのポリシーおよび手続きには、適用法および適用される団体協約により許可される範囲において、本書にさらに規定する就労資格の確認、雇用歴および犯罪歴のバックグラウンドチェック、ならびに雇用前薬物検査が含まれることを表明し、保証し、誓約するものとします。前述の一般性を制限することなく、サプライヤーはさらに、シティに配属されたすべてのサプライヤー人員がすべての移民関連適用法を完全に遵守し、任務期間中を通じて就労することを許可されていることを検証することを含め、サプライヤーがすべての移民関連適用法を完全に遵守するための管理および手順を有することを表明し、保証し、誓約するものとします。要請があった場合、サプライヤーは、シティに配属されたサプライヤーの人員の一部または全部の就労許可および移民関連適用法の遵守を証明する書面を速やかに提供し、適用法に従う就労許可を持たない人員を適任の代替人員と入れ替えるものとします。これには、適時かつ効果的にサービスを提供できるよう必要なすべての研修およびオリエンテーションを提供することを含み、それぞれの場合にシティに対する追加費用なしに行います。

7.4 サプライヤーの所有権

シティが事業を行う管轄区域の適用法および規制を遵守するため、シティからの要請に応じて、サプライヤーは自然人および/または事業体である所有者の詳細を提供する義務があります。これには、サプライヤーの直接的な所有者が含まれ、エンゲージメント、商品、またはサービスを通じて影響またはその他の手段を通じて直接または間接的に所有または管理を行う最終的な受益者が含まれます。

8 不正管理

不正リスクを特定し軽減するためのシティの取り組み（以下「不正管理」）に関連するもの。

8.1 すべてのサプライヤーは以下を行うものとします。

1. 窃盗、詐欺、その他の犯罪行為または不正行為の疑いまたは疑いに関するシティの調査、および不正行為または犯罪行為の訴追に、法律の及ぶ最大限の範囲で協力する。

2. 潜在的な不正インシデントを [Ethics Hotline](#) を通じて適宜シティに報告および言及する。これには、シティ、シティの従業員、シティのサプライヤーまたは代理人、シティの非従業員（派遣社員、契約社員など）が関与する窃盗、詐欺（サプライヤー、料金制度、資金または証券消失問題などに関する意図的に間違ったデータや不正確なデータを提供したり、虚偽報告したりすることなど）、犯罪活動、不正行為未遂、疑い、申立て、あるいは実際の当該行為が含まれますが、これらに限定されません。
3. シティおよびその代表者による監督および監視を許可し、そのサプライヤーが関与する潜在的な不正行為の調査をシティおよび法的執行機関が遂行できるように支援する。
4. サプライヤーが認識した利益相反（サプライヤー/サプライヤー従業員および/またはシティ従業員間の利益相反を含む）を適時に報告する。
5. シティのサプライヤー支払システムにおけるサプライヤーの銀行口座の設定または更新時に、シティの不正防止プロセスをサポートする。

8.2 これに加え、本質的に不正リスクにさらされやすいサービスを提供するサプライヤーは、以下を行う**必要があります**。

1. サプライヤーがシティに提供するサービスに関する重大な不正リスクを特定するための不正リスク管理プログラム、およびこれらのリスクを軽減するための管理および手順を文書化し、これに従う。
2. 不正認識トレーニング（入社後 90 暦日以内、それ以降は年に一度）を完了し、シティに提供される特定のサービスに特有の不正リスク要因に関する従業員研修を行う。
3. 不正未遂を監視し、シティに提供するサービスに関連する不正リスクを軽減する効果的な管理体制を維持し、管理体制の手順を文書化し、その効果を定期的に検証し、不備があった場合はビジネス活動担当責任者（BAO）に報告する。
4. ビジネス活動担当責任者（BAO）への不正リスクエクスポージャーのデューデリジェンス/継続的なモニタリング/評価に必要な情報を提供する。

5. デューデリジェンスには、不正リスク軽減に関連するサプライヤーの能力に関する統制評価を実行するように設計されたサードパーティ不正行為インパクト評価テンプレート（「TP-FIAT」）が含まれます。この業務手順では、ビジネス活動担当責任者（BAO）またはサードパーティ担当責任者（TPO）および不正行為リスク管理担当責任者（以下「FRMO」）が、不正リスクを特定および管理するための一連の手順について説明します。

8.3 本質的により高い不正リスクにさらされるサプライヤーには、以下が含まれますがこれらに限定されません。

1. 社内アカウント、金融取引、現金取引にアクセスするなど、不正に悪用される可能性のある「機密」または「極秘」（シティの直接の管理下または監督下でないもの）以上に分類されるデータにアクセスできる
2. シティのネットワークやシステムに接続できる
3. 以下を含む不正を行ったり、不正を可能にしたりするための標的となりやすい、サービスおよび機能を提供、サポート、またはアクセス権を保有している
 - a) 新規クライアントの本人確認、オンボーディング、または募集手続き。
 - b) シティまたはクライアントの決済/資金送金活動、および/またはシティのクライアントがこれらのサービスにアクセスする際の認証
 - c) シティのデータまたはシティのクライアントに関するデータ（人口動態など）の作成、確認、または変更
 - d) 取引手法（デビット/クレジットカード、eWallet、小切手など）の提供、サービス、または認証
 - e) 不正の防止、検出、または対応に関連する、業務上の違法防止策をシティに提供およびサポートしている
 - f) 現金、金融商品、および資産/物理的な物品への物理的なアクセスの提供
 - g) シティ施設内への付き添いなしまたは時間外の出入り
 - h) 財務諸表：GL/SL への記帳などの会計業務
 - i) インセンティブが伴う活動に対する報酬の獲得および使用

9 メディアへの対応と公式会見

シティのエンタープライズサービス・広報部は、シティのためのプレスリリースや公式な声明を発表することを許可されている唯一の部署です。サプライヤーはシティ、サプライヤーとシティとの間の契約または取り決め、あるいはサプライヤーからシティが調達した製品とサービスを直接的または間接的に特定するプレスリリースを発行することはできません。サプライヤーは、シティの主要連絡窓口からの書面による事前の同意なく、クライアント、シティ従業員、シティのその他サプライヤー、サプライヤーのその他の顧客、またはその他の第三者と、シティに関連する広報活動について同意したり、それに関与したりすることはできません。

サプライヤーは、シティの主要連絡窓口およびシニアカントリー広報担当者からの書面による事前の同意なく、シティ、シティの業務、クライアント、商品またはサービスに言及する書面または電子形式の資料（書籍、記事、ポッドキャスト、ウェブキャスト、ブログ、ウェブサイトへの投稿、写真、動画、ソーシャルメディア、またはその他のメディアを含む）を公開もしくは掲載する、それらについての演説を行うまたは演説を作成する、インタビューに答える、または公式の場に出る、といったことはできません。

シティへのサービスまたは製品の提供に関連するか否かを問わず、サプライヤーは、シティ独自の標識、商標、サービスマーク、商号、ロゴ、シンボル、またはブランド名のいずれの場合においても、シティの書面による事前の同意を得ることなく、それらを使用することはできません。サプライヤーは、シティの名称、ロゴもしくは商標、施設または取引関係を、シティ以外の利益のため、または業務のために利用することはできません（これにはレターヘッド、個人のウェブサイト、ブログ、またはその他ソーシャルネットワークサイトが含まれます）。さらにサプライヤーは、シティの名称、施設、または関係を、慈善目的または無料奉仕目的のために使用することはできません。

10 電子的な文書によるコミュニケーション

シティの従業員とやり取りしたり、シティのためにまたはシティに代わって義務を遂行したりする際に、サプライヤーはシティが承認した書面による電子通信機器、システム、およびサービスのみを使用することができます。新規、拡張または変更されたシティの電子コミュニケーションチャネルは、スタンドアロンツールであるか、シティまたは第三者が提供する広範なプラットフォームに統合されているかを問わず、該当するシティの要件に従って、またはサプライヤーに宛てた BAO からの書面での通知により、承認されるものとします。WhatsApp、WeChat、LINE、Slack、Signal、Telegram、iMessage、SMS、Viber その他のインタラクティブ電子プラットフォームなどシティに承認されていないメッセージングプラットフォームでシティ従業員とシティとの取引について連絡することは禁じられています。

また、サプライヤーは、シティが提供した通信機器、システム、およびサービスを介して作成、開示、使用、アクセス、ダウンロード、保存、送信、受信、または削除された電子的な文書によるコミュニケーションについてはプライバシーを期待すべきではありません。シティは、電子通信機器、システム、およびサービス、ならびに電子コミュニケーションを監視することがあります。このような電子コミュニケーションはシティが所有し、適用される記録保持要件に従って（現地の法規制を条件に）保存することができます。

<https://policydirectory.citi.net/cpd/ layouts/15/DocIdRedir.aspx?ID=CPDPROD-13-8739>

11 政治活動と献金

外国の影響力、選挙資金、贈答品および接待、議員・草の根・親善・規制担当者へのロビー活動、購買、ペイ・トゥー・プレイ（支払いを条件とする参加）、証券などに関するさまざまな法律により、シティおよびそのサプライヤーによる政治活動、ならびに当該活動に関連する情報開示が規制されています。関連するシティのポリシー、基準、または法令に準拠しないサプライヤーの政治活動は禁止されています。

政治活動には以下が含まれますが、これらに限定されません。

1. 公職、政党委員会、もしくは政治委員会に向けた選挙運動を行っている候補者のために、企業または個人の政治献金を行う、政治献金を勧誘する、または会社の資金

もしくはリソース（施設、機器、ソフトウェアまたは従業員など）を使用したり、業務時間中に個人的なサービスを任意で提供したりすること

2. 直接的に行うか第三者を通じて行うかに関わらず、ロビー活動または役人に働きかける活動に関与すること（これには役人や立法に影響を及ぼす試みが含まれ、管轄区によっては、行政機関規則制定または政府契約の入札に影響を及ぼす試みが含まれる場合もあります）
3. 政府関連の公職に出馬、就任する、またはその任期を務めること（政府の評議会、委員会、または他の類似した組織を含む）

シティの政府関係業務グローバルオペレーションコントロール（ggacontrol@citi.com）からの書面による事前の承認なしに、シティまたはそのクライアントのために（または意図的にシティに代わって）サプライヤーが政治活動を引き受けたり実施したりすることはできません。シティは、ロビー活動など、サプライヤーが提供する、契約済みで許容範囲内の政治活動サービスに対して手数料を支払ったり、自費で払い戻しを行ったりすることができますが、個人または企業の政治献金についてはいかなる種類のものであっても、シティがサプライヤーやその従業員に払戻しを行うことは一切ありません。

12 マネーロンダリング対策（「AML」）

適用対象：サプライヤーが特定の顧客関連サービス（オンボーディング、顧客アカウントや取引のスクリーニング）を行う際、または前述の活動に関連したデータ/メトリクスの送信時、および/またはサプライヤーが金融取引または商品（オンラインデポジット、宅配便、現金輸送車、または金庫サービス、電信送金、デジタル資産など）関連の仲介を務める場合

12.1 AML の義務：

1. シティのプロセスおよび適用法の遵守

- (i) グラムリーチブライリー法とその下に公布された規制、(ii) 米国愛国者法とその下に公布された規制、(iii) マネーロンダリングに対処するすべての法令、および(iv) 経済制裁に関連するすべての法令を含む、適用法

の要件に対処するためのシティのプロセスおよび手順を維持し、遵守するものとします。かかるポリシーおよび手順は、金融活動、金融取引、現金の受け取りに関連して異常と思われる、または異常である可能性があるとして認められた活動を直ちに報告する要件を含め、マネーロンダリング対策の役割と責任に対処するものです。

2. 人員のための年次トレーニングおよびプログラム要素：

- シティにサービスを提供するその従業員にマネーロンダリング対策の役割と責任に関する年次トレーニングを確実に受けさせること。トレーニングには、金融活動、金融取引、現金の受け取りに関連して異常と思われる、または異常である可能性があるとして認められた活動を直ちに報告する要件が含まれます。トレーニングの構成要素として以下のようなものが挙げられますが、これらに限定されるものではありません。
 - a.疑わしい活動の報告およびエスカレーション
 - b.「顧客の身元確認」（CIP）プログラム、制裁措置と名前の照会、顧客のデューデリジェンス（CDD）、強化されたデューデリジェンス（EDD）、および**最終的な実質所有者（UBO）**の特定と検証を含む「Know Your Customer（顧客を知る）」（KYC）プログラム
 - c.関連するすべての金融商品およびアクティビティに対する取引モニタリング
 - d.法律および規制変更、および AML プログラムの重大な変更についての報告を含む、定期的な報告/メトリクス
 - e.現地視察を含む、AML プログラムの効果検証および管理

3. 契約条項の遵守：

- サプライヤーが制定しなければならないプログラムを定義する契約条項を遵守すること

4. 疑わしい不履行の速やかな報告：

- 法律違反の疑いを直ちに書面にてシティに報告すること。これには、シティまたはその顧客に関連する金融活動、金融取引、現金の受け取りに関連して、異常と思われる、または異常である可能性があると思われる活動が含まれます。

5. 脱税の防止と通報：

- 事業を行う国で適用されるすべての税法および規制を遵守すること。
- いかなる場合でも、サプライヤーは、納税義務のある税金の支払回避を支援する行動への関与や、税務当局に対する情報隠蔽をはじめとして、意図的に違法な脱税を行ったり、他者のためにかかる脱税の手助けをしたりしないものとします。
- そのため、サプライヤーは脱税に関連する妥当な予防手段を採択し、シティに関連する違反や違反の疑いをシティに書面にて速やかに報告するものとします。

12.2 サプライヤーの社内ポリシーおよび手順

サプライヤーは、現在施行されている、または今後施行されるすべての AML 法および規制を遵守するために、適切な社内ポリシーと手順を維持するものとします。

13 記録管理

適用対象：シティの情報のアクセス/処理/保管を行うサプライヤー

シティは、シティの情報を保管する全サプライヤーに対し、それぞれのビジネス活動担当責任者（「BAO」）またはシティの主要連絡窓口と協力して、(i)シティの記録管理目的のために情報を記録または一時的な情報として識別し分類、(ii)マスター記録カタログ（「MRC」）に従って記録を分類、(iii)保持要件に基づいて情報を保持、および

(iv)情報保留が指定されていない場合は、情報ライフサイクルの終了時に情報を適切に処分することが義務付けられています。

BAO またはシティの主要連絡窓口は、サプライヤーと協力し、サプライヤーが MRC のシティ記録コードに従って記録を識別し分類し、インベントリが少なくとも年 1 回更新されることを確実にする必要があります。サプライヤーには、BAO から通知された記録管理要件に従う義務があります。処分の資格基準を満たす記録は、情報保留の対象である場合を除き、できるだけ早く適切に処分する必要がありますが、保持要件が満たされてから 6 か月以内に処分する必要があります。一時的な情報は、情報保留の対象でない限り、最後に使用してから 2 年以内に破棄するものとします。個人情報が含まれた一時的情報は、情報保留の対象でない限り、収集した目的が満たされた後は削除しなければなりません。サプライヤーは、情報保留を通知された場合、シティの情報の破棄または変更を中止するものとします。不明な点がある場合は、サプライヤーはシティの主要連絡窓口または BAO に問い合わせる必要があります。

四半期ごとに、国別保持スケジュールに列挙された保持規則を見直し、DRIM による規制および社内変更に準拠するために必要に応じて更新します。サプライヤーに影響を与える変更がある場合、BAO はサプライヤーに助言します。サプライヤーは影響を評価し、各システム、プロセス、インベントリーに変更を実装する必要があります。BAO からの通知を受けてから 90 日以内に、自社が所有・管理する記録の種類を特定します。

シティに代わって文書を管理するサプライヤーは、法的またはその他の手続きに関連するとみなされるすべての情報を、BAO の要求に従って必要な期間内に保存（「保有」）、収集、および提供する責任を負います。サプライヤーは、要請があった場合、適用される契約条件に基づき要求されるシティの情報を返却しなければなりません。サプライヤーは、情報の分類（機密、非機密など）を問わず、シティの主要連絡窓口または BAO の承認なしに、いかなるシティの情報も破棄してはなりません。この承認には、処分予定の情報に有効な情報保留が適用されていないことの確認が含まれます。記録管理と保持要件およびその他すべての情報取扱い要件は、明示的に別途合意されている場合を除き、契約の終了または満了後も存続するものとします。

サプライヤーは、サプライヤーが保管するシティの情報の管理を監督する責任を担う。サプライヤーの従業員の全員を記載した文書を維持するものとし、連絡先氏名、手順の詳細、役割、責任、およびシティのサプライヤー記録インベントリの見直しと更新を行うために、それぞれのシティの主要連絡窓口または記録管理責任者と定期的なミーティングを持つものとし、ます。

14 ビジネスのエンタープライズレジリエンス/継続性

適用対象：シティが使用するサービスまたはホストテクノロジーのインフラストラクチャ/アプリケーションを提供するサプライヤー。適用対象およびビジネスの持続性（CoB）要件をサプライヤーに通知することは、シティビジネス活動担当責任者（BAO）の責任

14.1 復旧リソース

サプライヤーの災害復旧計画では、サプライヤーの主要な施設が使用不能となった場合に、シティにすべての製品とサービスを提供できる代替リソースを規定するものとし、ます。復旧リソースは、同じ災害事象が主要施設と復旧場所の両方に影響を与える恐れを最低限に抑えるか、それを排除するために十分な距離間隔がある、主要施設から地理的に分離された場所に存在する必要があります。

1. 復旧リソースは情報システムに限定されず、シティに対する製品とサービスの継続的な提供に必要なリソースがすべて含まれます。これには、スタッフ、建物、ビジネス機器、データセンター、データおよび音声ネットワーク、輸送サービスなどがあります。
2. アプリケーションのサプライヤーは、高可用性（HA）の設定を確保するために、Hot/Hot タイプのアーキテクチャを実装することができます。このアーキテクチャでは、クライアント/ユーザーが起動して実行できる（最低でも）2つの同一構成のシステムがあることが求められています。このモデルが提供する最も重要な特徴は、代替環境がプライマリ（実稼働）データセンターと同時に稼働していることです。

14.2 復旧サービスレベル

サプライヤーのビジネス継続性は、シティに対して効果的であるように、設定済みのサービスレベルを満たさなくてはなりません。サプライヤーの災害復旧計画は、最低限、以下の変数に対する具体的な数値を定めるものとします。

1. 目標復旧時間
2. 目標復旧時点
3. 復旧リソース/テクノロジー能力
4. 復旧期間

14.3 災害復旧計画

サプライヤーは、特定の場所から、または特定の個人の努力により本契約に基づく本商品またはサービスを提供する、またはその他の義務を履行するサプライヤーの能力が中断された場合でも、サプライヤーが速やかに別の場所からまたは代替りの人員により本商品またはサービスの提供および義務を履行できるように、事業継続のための災害復旧計画を維持し、シティが要求する場合はその最新の定期テストの証拠を提出するものとします。災害復旧計画のコピーは、シティとサプライヤーの間で締結された各作業指示の発効日から 10 暦日以内に、またその後各作業指示が有効である限り毎年シティに提供されなければならないものとします。サプライヤーは、サプライヤーが災害復旧計画を発動する状況下で、シティがサプライヤーから本商品またはサービスの提供を継続するために必要な指示またはその他の情報をシティに提供するものとします。サプライヤーは、災害復旧計画に最低限次の事柄を含めることを表明し、保証し、誓約するものとします。

1. テクノロジーを利用できない（サービス拒否/DoS）、主要な勤務地を利用できない（アクセス拒否/DoA）、スタッフを利用できない（業務委託先を含む）を含む混乱の影響を軽減するための移転、業務の移転、および/またはリモートアクセスを含む復旧手順および戦略
2. サプライヤーによる本商品またはサービス拠点とは別の二次災害復旧拠点の維持、本商品またはサービス拠点とは別の場所でのバックアップ媒体の保管、通信回線やサーバーの二重化など（これらが挙げられるが、これらのみに限定されない）
3. 停電、システム障害、自然災害、その他の不測の事態による商品またはサービスの長期中断に対応するための詳細かつ文書化された計画で、相

互に合意した期間内に業務を再開するためのプロセスと手順を含む、商品またはサービスの運用および適用のバックアップ/復旧のための手順

4. すべてのコンテンツを保護するための手順
5. 交換用機器（コンピュータ機器など）に関する手順および第三者との契約
6. オフサイトの生産施設のための手順、および
7. サプライヤーの災害復旧計画では、以下を実行します。
 - a. サプライヤーは、商品またはサービスに悪影響を及ぼす可能性のある災害を速やかにシティに通知します。
 - b. サプライヤーは、当該通知から 24 時間以内に、代替処理施設において商品またはサービスの提供を継続する計画をシティに提供します。
 - c. 本商品またはサービスは、要求される目標復旧時間（RTO）内に完全に稼動するものとします。契約の中で RTO が別途定義されていない場合、RTO は、シティによって重要度が「エンタープライズ・クリティカル」または「高」と定義されている場合の障害復旧は 4 時間以内、シティによって重要度が「中」と定義されている場合は 24 時間以内、シティによって重要度が「低」と定義されている場合は 72 時間以内に災害復旧するものとします。および
 - d. サプライヤーの施設の一部が稼動不能となった場合、サプライヤーはシティに対して、サプライヤーが他の商業顧客に対して行うのと同様に、不利な扱いをしないものとします。

14.4 ホスティングサービスに適用される災害復旧計画要件

サプライヤーがシティにホスティングサービスを管理し、提供する限りにおいて、以下の規定も適用されるものとします。災害復旧計画に最低限、次の事柄を含める必要があります。

1. 停電、システム障害、自然災害、その他の不測の事態によるサービスの長期中断に対応するための詳細かつ文書化された計画で、相互に合意し

た期間内に業務を再開するためのプロセスおよび手順を含む、ホスティングされたサービスの運用および適用のバックアップ/復旧のための手順

2. さらに、サプライヤーの災害復旧計画では、以下を実行します。(a) サプライヤーは、サービスに悪影響を及ぼす可能性のある災害が発生した場合、2 時間以内にシティに書面にて通知します。(b) サプライヤーは、当該通知から 24 時間以内に、代替処理施設においてホスティングされたサービスの提供を継続する計画をシティに提供します。および(c) ホスティングされたサービスは最初の通知から 48 時間以内に完全に機能しているものとしします。
3. サプライヤーは要請に応じて、シティがサプライヤーの災害復旧計画およびビジネス継続計画と連携して災害復旧計画およびビジネス継続計画を策定するために必要な情報を開示することに同意するものとしします。および
4. サプライヤーの施設の一部が稼働不能となった場合、サプライヤーはシティに対して、サプライヤーが他の商業顧客に対して行うのと同様に、不利な扱いをしないものとしします。

14.5 災害復旧計画への変更

サプライヤーは、(RTO の長期化など) サービスに悪影響を及ぼす可能性のある方法で災害復旧計画を改悪させない限り、その災害復旧計画を変更することができます。サプライヤーは、災害復旧計画の変更を速やかにシティに伝え、シティの要求に応じて、シティが十分に理解し、変更に対応できるよう説明するものとしします。

14.6 業務委託先の災害復旧計画

サプライヤーは、サプライヤーの業務委託先が、シティがサプライヤーに求める要件と完全に一致する災害復旧計画および関連する事業継続管理措置を維持することを保証するものとしします。サプライヤーは、業務委託先に対して適切な監督を行い、その管理体制や試験結果の定期的な確認を含め、特定された不備については速やかに是正措置を講じるよう確保しなければなりません。

14.7 災害復旧計画の呼びかけと危機の通知

サプライヤーは、シティの主要連絡窓口以下に以下の事柄を速やかに通知します。

1. サプライヤーが災害復旧計画を発動した場合

2. シティに提供されるサービスまたは商品に悪影響をもたらす可能性が疑われるサプライヤーや業務委託先に対する危機、脅威、警告、またはサイバーイベント

14.8 テスト

サプライヤーの復旧リソースおよび計画はすべて、本番導入後 120 日以内に（シティが「エンタープライズ・クリティカル」として分類したアプリケーションの場合、90 日以内）テストし、少なくとも年 1 回（12 か月ごと）テストするものとします。テストでは、シティに提供するすべての製品とサービスの復旧サービスレベルを満たすサプライヤーの能力を実証するものとします。これらのテストは、包括的なものでなければならずシティに提供された本サービスの全範囲を含むものでなければなりません。サプライヤーは、シティに提供する商品またはサービスの復旧テストについて少なくとも 30 暦日前までにシティに通知しなければなりません。シティは、復旧環境におけるアプリケーションのビジネス機能を検証するために、シティが使用するアプリケーションのサプライヤーによる復旧テストに参加または観察することができます。シティが参加を希望する場合、サプライヤーは、テストの実施前に、テストの目的、テスト計画、テストサイトへの接続手順などをシティに提供するものとします。各テスト完了後、10 営業日以内に、サプライヤーは、回復に必要な時間枠およびテスト結果の証拠（スクリーンショットなど）を含む、テスト目的、テスト計画、およびテスト結果の概要をシティに提供するものとします。

14.9 ボリュームの検証

シティが「エンタープライズ・クリティカル」と分類したアプリケーションをホスティングするサプライヤーは、実稼働量を COB/災害復旧環境で処理できることを実証しなければなりません。シティとサプライヤーは、検証に使用される方法について合意するものとします。

14.10 サービス提供のためのシティのシステムの使用

シティまたはシティの関連会社から要請があった場合、シティのシステムを使用するサプライヤーは、シティの災害復旧訓練に、シティに費用または料金を負担させることなく参加するものとします。

14.11 テスト結果への対応

サプライヤーのテスト結果の中に、テストの目標または該当する RTO が満たされなかった旨が記されている場合、サプライヤーは原因分析を行い、特定された不具合を速やかに修正するものとします。かかる修正を適用後、サプライヤーは初回のテストに不合格（または、関連の作業指示書に明記された期間）後、120 暦日（シティが「エンタープライズ・クリティカル」と分類したアプリケーションの場合、90 暦日）以内に再テストを実施するものとします。

14.12 危機管理

サプライヤーは、ビジネス継続計画と併せて、復旧作業の指揮統制のための危機管理計画も維持するものとします。最低でも、サプライヤーの危機管理プランは、復旧業務を開始する十分な権限のある個人を特定し、危機情報を収集および拡散するための通信およびエスカレーションプロトコルを定義して、危機が生じた場合にシティと連絡するための通知およびエスカレーションプロトコルを含むものとします。

14.13 業務継続の評価

サプライヤーは、シティ要件ならびにビジネス継続性に関連する法律および/または規制要件（シティまたはサプライヤーに適用されるもの）の遵守に関して、サプライヤーのポリシー、手順、統制を評価するシティの第三者ビジネス評価プロセス継続性の対象となります。この評価は、裏付けとなる証拠を伴うサプライヤーの回答を要するアンケートで構成されており、サプライヤーの拠点への訪問が含まれる場合があります。評価の結果により問題と懸念事項が明らかになった場合、シティは結果を文書化し、サプライヤーと協力して、問題の修正方法を特定します。サプライヤーは、シティの懸念事項に対し合理的に満足できる状態で対処するため、迅速に必要な是正措置を講じる、および/または補完的な管理措置を追加しなければなりません。

14.14 オペレーショナル・レジリエンス

重要なビジネスサービスとは、その提供が中断された場合、シティ、クライアント、または金融システムに重大な悪影響を及ぼす可能性のあるサービスです。サプライヤーは、シティが随時指定する重大なビジネスサービスに相当する、またはシティによる重大なビジネスサービスの提供のサポートとなる（以下「重大なビジネスサービス」）本サービスの要素の提供に対する障害は、シティがサプライヤーに随時通知する、シティが設定する期間を超過、またはシティが定める何らかの関連指標（以下「インパクトトレランス」）に違反しないことを保証するものとします。インパクトトレ

ランスは、サービス提供が中断される可能性のある時間に相当する、明確な時間的基準として表されます。シティとサプライヤーは、継続的な契約ガバナンスプロセスの一環として、インパクトトレランスを毎年見直すものとします。複数の規制機関の要求により、個々の重大なビジネスサービスに対して複数のインパクトトレランスを設定する必要がある場合、シティは、当該重大なビジネスサービスに対して個別のインパクトトレランスを指定することができます。サプライヤーは以下を行うものとします。

1. シティが設定した該当するインパクトトレランス内で、サービスを提供できない（またはその可能性が高い）ことを認識した場合、見込みまたは実際の失敗の理由およびその影響を緩和するために講じている措置についての説明と共に、直ちにシティに通知すること。
2. 要請があった場合、サプライヤーが重大なビジネスサービスをサポートするあらゆるサービスを提供するために必要な人材、プロセス、技術、施設および情報をシティが特定できるように、シティに合理的な支援を提供すること。
3. シティが以下を実施できるように、シティに合理的な支援を提供すること。
 - a. サプライヤーまたはサプライヤーの業務に、深刻だがもっともらしい障害が発生した場合、サプライヤーが各重大なビジネスサービスのインパクトトレランス内にとどまる能力に関する内部シナリオテスト
 - b. シティがサプライヤーの弱点を特定し、将来の混乱に効果的に対応し回復するサプライヤーの能力を向上させるために必要な行動を可能にする、シナリオテスト後に実施された教訓

シティによる内部シナリオテストにおいて、シティが設定した、対応するインパクトトレランス内でサービスを提供するサプライヤーの能力に対する脆弱性または制限が特定された場合、およびサプライヤーが、シティが設定したインパクトトレランス内でサービスを提供できなかった場合、当事者は、サプライヤーが当該脆弱性または制限を解決もしくは緩和するために必要な措置を講じる、またはこの失敗の原因を改善して合理的に実行可能な限り速やかにインパクトトレランス内に留めるよう

にすることを確実にします。（該当する場合）

14.15 エスクローの手配

シティの要請により、サプライヤーは、(i)シティ環境内での操作についてシティにソフトウェアをライセンス供与するか、(ii)ホスティングサービスをシティに提供する場合、預託物がシティの指定するエスクローエージェントに預託されていることを確認し、該当するエスクロー契約に基づき、預託物に関してエスクローエージェントが要求する預託者登録表またはその他のフォームを実行するものとします。その後、ライセンスまたはホスティングサービスに関して適用される契約の残りの期間を通じて、サプライヤーは、エスクローエージェントに更新された預託資料を預託し、エスクローされたソースコードおよびその他の預託資料が、シティが使用しているソフトウェアまたはホスティングサービスのバージョンに適用される最新のバージョンのソフトウェアで常に最新の状態であることを保証するものとします。ソースコードまたはその他の預託資料の更新は、シティに使用許諾されたソフトウェアへの更新またはシティが使用しているホスティングサービスの変更があった日から 30 日以内に、エスクローエージェントに交付されます。サプライヤーは、エスクロー契約に定める預託者のすべての義務と要件を完全に遵守します。サプライヤーは、設定料金、年会費、預託料金、サービス料金、およびその他のエスクロー料金および費用を含むがこれに限定されないすべてのエスクロー費用および料金についてのみ単独で責任を負います。公表事由が発生した場合、エスクローエージェントは、基本合意およびエスクロー契約条件に従い、預託資料をシティまたはシティの指定する者に公表するものとします。ソースコード（またはその他の預託資料）がシティまたはシティの指定する者（該当するエスクロー契約に基づく義務の履行においてサプライヤーまたはエスクローエージェントが直接提供する）に引き渡される場合、ソースコードおよび預託資料は、サプライヤーとシティとの間の関連する契約に基づく既存のライセンスの対象となります。ただし、各ライセンスは、以下を実行するために合理的に必要であると、シティにソースコードおよびその他の預託資料を使用および変更する資格があるとみなされます。(i)当該ソフトウェアおよびその他の預託資料をシティのシステムと統合し、互換性を確保すること、(ii)当該ソフトウェアまたはその他の預託資料が適用法、業界基準、市場慣行に適合させること、(iii)当該ソフトウェアまたはその他の預託資料が技術革新により現在維持されていること、および(iv)当該ソフトウェアおよびその他の預託資料が既存のライセンスの範囲内でシティおよびその関連会社のビジネス目的を果たすことを可能にすること。ソースコードを使用してシティによってまたはシティに代

わって開発される変更を含むソフトウェアのいかなるバージョンも、本セクションのすべての規定および基本となる契約の対象となります。ただし、サプライヤーにはいかなる変更に対する権利、権原または持分がなく、変更に対するすべての知的財産権はシティに排他的に帰属するものとします。

サプライヤーは、サプライヤーがソースコード預託に当該第三者のソフトウェアのソースコードを配置できるようにするため、ソフトウェアに使用されるソフトウェアを提供した第三者と商業的に合理的な努力を払うものとします。第三者がサプライヤーにこの権利を付与することを拒否した場合、サプライヤーは公表事由において、該当する第三者のソフトウェアライセンス契約をシティに譲渡できるよう、商業的に合理的な努力を払うものとします。

本項に従ってシティに提供するソースコードは、シティが事業および業務要件に関連してソースコードおよびソフトウェアを使用し、変更し、本ソフトウェアが技術革新により現在にとどまり、適用法を遵守できるようにすることを条件として、該当するライセンスされたソフトウェアまたはホスティングサービスの既存のライセンスの対象となります。ソースコードを使用してシティによってまたはシティに代わって開発される変更を含むソフトウェアのいかなるバージョンも、該当する契約のすべての規定の対象となります。ただし、サプライヤーにはいかなる変更に対する権利、権原または持分がなく、変更に対するすべての知的財産権はシティに排他的に帰属するものとします。

15 身元調査のグローバル基準

適用対象：シティにサービスを提供するすべてのサードパーティーサプライヤー

15.1 概要 – 身元調査

身元調査は、適用されるすべての現地の法律および規制に従って実施する必要があります。サプライヤーの代表者、サプライヤーの従業員および業務委託先は適宜、本書で説明されている情報と自己開示内容のすべてを提供しなければなりません。履歴書、面接時、入社承諾書、または入社プロセス中などに情報を改ざんまたは省略した場合、発覚時期を問わず、現地の法律に従い、シティとの取引の拒否または中止の原因となる場合があります。実施された調査の結果がよくなかった場合も、発覚時期を問わず、現地の法律に従い、シティとの取引の拒否または中止の原因となる場合があります。

ます。

身元調査の完了に関する追加情報は

https://www.citigroup.com/rcs/citigpa/storage/public/country_background_screening_requirements_tables.pdf で確認できます。

15.2 基本情報の収集および本人確認

サプライヤーの従業員がシティの職務を開始する前にサプライヤーは個人の氏名、郵送先住所、本籍地（異なる場合）、電話番号、電子メールアドレス（該当する場合）を収集しなければなりません。サプライヤーの従業員は、自らの身元を検証する文書も提供しなければなりません。これには、国民 ID 番号、政府発行の写真付き身分証明書、パスポートなどの情報および/または書類の提供が含まれる場合があります。

15.3 制裁審査

シティのデータ/システム/ネットワークへのアクセスおよび/またはシティ敷地内へのアクセスにかかわらず、業務委託先を含む、シティの代理として業務を行うすべてのサプライヤーの従業員、またはシティのベンダーの 25%以上の株式を保有する所有者は全員、米国財務省外国資産管理局（「OFAC」）の特定国籍業者リスト（「SDN リスト」）および米国が課す制裁の対象地域および管轄区域のリスト（「米国制裁」）に加え、欧州連合（EU）統合金融制裁リスト、国連（「UN」）安全保障理事会統合リスト、英国（「UK」）制裁リスト、および当該地域の管轄区域に適用される法令に基づくリスト（「非米国制裁」）など、米国以外の当局が発行したあらゆるリストおよび制裁対象となる管轄区域の名称に照らして審査されなければなりません。

OFAC リストは、こちらのウェブサイトで公表されています：

<https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

15.4 移民法コンプライアンス

サプライヤーは、すべての人員が配属先の国で就労する許可を得ていることを確認するための手順を整備し、実施していることを証明しなければなりません。さらに、サプライヤーは、(1) 全従業員が就労許可を得ていることを確認し、(2) すべての適用法令および方針（就労資格および確認要件を含む）の遵守を維持しなければなりません。サプライヤーはさらに、その従業員がその他の点ですべての適用される移民法および規制に準拠している状態を維持しており、その従業員が従事する任務および活動に対

して適切な資格や分類のビザを保持していることを確認するための手順を備えていることを証明しなければなりません。

15.5 職歴

サプライヤーは、その従業員の過去7年間、または現地の規制により義務付けられる場合は過去10年間の職歴を確認するものとします。個人の職歴を検証して、雇用主、役職、日付、および職務が正確に記載されていることを確認する必要があります。サプライヤーの従業員は、シティまたはその前身企業（シティバンク、シティコープ、トラベラーズ、ソロモン・ブラザーズおよび/またはスミスバーニーが含まれるがこれに限定されない）へのコンサルタントまたは契約社員としての以前の雇用または派遣についても開示する必要があります。

15.6 学歴

サプライヤーは、その従業員の最終学歴を確認するものとします。確認情報には、在籍期間、教育機関名、住所、取得学位が含まれます。

15.7 犯罪歴

法的に許可される場合、サプライヤーの従業員または再委託業者は、有罪の申し立てまたは不抗争答弁、または公判前ダイバージョンおよび同類のプログラムへの参加を含む、刑事犯罪における逮捕、出頭命令、召喚、罪状認否、起訴または有罪判決の対象となった場合、その旨をシティに開示しなければなりません。犯罪歴のレビューおよび/または指紋照合は、法律で許可され、かつ利用できる場合、職務開始日の前に完了する必要があります。盗難、詐欺、不正行為、背任に関連した有罪判決、または現地の法律で定義されている類似の違反（法律で禁止されている場合は除きます）により、シティでの職務遂行の拒否および/または職務適格性喪失につながる可能性があります。その他の前科がある場合、適用される現地の法律や規制に基づき、職務遂行の拒否および/または職務適格性喪失につながる可能性があります。

15.8 再審査

配属が終了したサプライヤーの従業員が再度シティに配属される場合、その従業員を再審査する必要があります。再審査要件の詳細情報については、https://www.citigroup.com/citi/suppliers/data/background_screening_requirements_tables.pdfにある各国特有の要件と例外を参照してください。

15.9 海外赴任

審査はすべて、従業員が赴任する国の規制に従って実施する必要があります。サプライヤーの従業員が新しい国に異動する場合は、新しい国の要件に従って個人を再審査する必要があります。

16 経費

事業活動費の払い戻しを請求する契約上の資格があるサプライヤー

16.1 概要

シティは、シティが書面により事前に承認し、該当する契約の条件に基づくシティへの製品とサービスの提供に関連するもので、適切な場合は該当する契約またはシティの業務経費ガバナンスポリシーとその関連する基準および手順の条件に従い、裏付けとなる領収書、請求書、旅程表、またはシティが認めるその他の証拠書類により十分に立証される、サプライヤーが負担した業務関連の合理的な経費のみについて払戻しを行います。

16.2 払戻し

これらの経費は適切に文書化し、シティの請求要件に従ってシティに請求書を提出するものとします。サプライヤーの経費は、サプライヤーに代わってシティの従業員が負担してはなりません。有効かつ承認された経費項目の払戻しのためシティに提出される経費には（その他のすべての請求要件に加えて）以下を含めてください。

1. 経費の事業目的
2. 経費の金額と内容
3. 経費の発生場所と日付
4. サプライヤーがサービスを提供するプロジェクトの名前/内容
5. 当該経費が生じたサービスを依頼したシティ担当者の氏名と取引関係
6. 該当する場合は、発注書番号

経費として認められる営業経費については、シティの主要連絡窓口にお問い合わせください。払戻しの請求と共に、裏付けとなる領収書、請求書、旅程表、またはシティが認めるその他の証拠書類の提出が必要です。払戻しの請求は、適切な場合は該当す

る契約またはシティの営業経費管理ポリシーおよび関連する基準および手順の規定に準拠し、また適切なビジネススポンサーおよび/またはシティの主要連絡窓口の承認を受け、対応する商品について十分な金額を有する個人により承認される必要があります。これに従わない申請については払戻しが行われません。

17 情報セキュリティ (IS)

適用対象：付録で分類・定義されているシティ情報のアクセス/処理/管理/保管を行う、およびインターネットに接続するシティブランドアプリケーションをホスティングする、およびシティのネットワークリソースに接続する、およびシティのネットワークリソースに接続する、およびシティ施設に同伴者なしでアクセスする必要があるサプライヤー

17.1 概要

本項では、シティの情報を保管、処理、管理、アクセスしたり、シティのアプリケーションをホスティングしたりシティへのネットワーク接続ができたりするベンダーのサブ処理業者または業務委託先を含むシティのサプライヤーに対し、シティが期待する最低要件について規定しています。これらの要件は、シティとそのサプライヤーが業務を行っている場所に適用法令の要件と最高レベルの業界基準（ISO / IEC 27001/2 など）に従って情報が保護されることを保証するものです。現地の法令、または関連のある業界基準が本書の規定よりも厳しく設定されている場合、サプライヤーはこれらの法令または基準に従う必要があります。さらにサプライヤーは、他のシティポリシーや契約条件の遵守の一環として、さらなる情報セキュリティ慣行および手順を取り入れるよう求められることがあります。サプライヤーが情報セキュリティのために追加セキュリティ慣行または手順を実施することを決定する場合、サプライヤーは、これらの慣行および手順が本セクションで定義される最低規制と矛盾しないよう確認する必要があります。

17.2 情報セキュリティ方針とガバナンス

サプライヤーは、情報セキュリティポリシーおよび基準を文書化しておく必要があります。方針ガバナンスには、明確に定義された役割と責任、およびテクノロジー、業界基準、法規制上の要件の現状との整合性を保つための、年次方針および基準の年次審査と更新が含まれていなければなりません。

17.3 職務の分離

サプライヤーは、承認または検知なく、同じ活動、変更、情報システム、または取引に対して常時アクセス権限があり、シティの情報にアクセスできる個人が、2つのビジネス機能または2つのIT機能、または2つの規制情報システム機能を遂行できないようにプロセスを設定する必要があります。ただし、リスクを緩和するための十分な補正管理策が講じられている場合は除きます。

表 A

部門	部門の説明
開発・エンジニアリング	ソフトウェア、ハードウェア、および構成の設計、作成、または変更。例としては、次のようなものがあります。 - 新しいアプリケーションコードと関連するデータベーススキーマの設計と作成 - インフラストラクチャ製品およびアプリケーションコンポーネントの設計 - ソフトウェアやサービスと連携できるよう、テクノロジー製品をカスタマイズ
承認	実装予定のコード変更の促進を承認する
システムの実装・運用	ソフトウェア、ハードウェア、および設定の変更のインストール、展開、または管理。 例としては、次のようなものがあります。 - 本番環境インフラへのコードの自動または手動によるリリースを実行 - テクノロジー製品またはアプライアンスのインストール - 本番データが格納されているシステムのトラブルシューティングおよび復旧作業を支援するためのサービスの起動または停止

特権 ID のアクティビティの確認	変更管理活動やセキュリティ関連のシステムイベント（監査証跡など）の検証
ID の管理	ID（ユーザー、FID、ボット）、権限、またはパスワードの追加、変更、削除
事業部門	部門の説明
ビジネス取引の開始	ビジネス取引を開始（「入力」「作成」「生成」とも呼ばれる）し、顧客情報を変更する
ビジネス取引の承認	ビジネス取引の承認（「認可」「確認」「承認」とも呼ばれる）
IT 部門	部門の説明
ネットワークオペレーション	ネットワークインフラストラクチャサービスを提供する製品の、デバイス管理および運用サポート。 ネットワークルーター、スイッチ、ファイアウォール、およびドメインネームサービス（DNS）などがその例
ネットワーク外オペレーション	ネットワークインフラストラクチャサービスを提供しない製品の、デバイス管理および運用サポート。サーバー、電話、コンピュータなどがその例

17.4 情報セキュリティに対する経営陣の責任

インターネットに接続するシティブランドアプリケーションをホスティングするサプライヤー、および/または機密またはそれ以上のカテゴリに分類されるシティの情報にアクセス権を持つサプライヤーは、シティ要件ならびに情報セキュリティに関する法律および/または規制要件（シティまたはサプライヤーに適用されるもの）の遵守に関して、サプライヤーのポリシー、手順、統制を評価するシティの第三者情報セキュリティ評価プロセス（TPISA）の対象となります。

この評価には、裏付けとなる証拠を伴うサプライヤーの回答を要するセキュリティアンケート、機密またはそれ以上のカテゴリに分類されるシティの情報が、第三者が保管、処理、および管理し、アクセスする第三者の施設への訪問が含まれます。さらに、TPISA 第三者継続モニタリングチームは、一般公開されている情報を活用して、サポート終了（EOL）ソフトウェア、悪用されたオープンポート、脆弱性、その他の侵害などの脆弱なインターネット対応のシステム、ホスト、アプリケーション、サーバーを特定するサイバーセキュリティモニタリングツールを使用してサプライヤーをモニタリングすることができます。TPISA の結果によりセキュリティの欠陥が開示または指摘された場合、シティはサプライヤーへの通知にて結果を文書化し、サプライヤーと協力して、これらの欠陥の是正方法を特定します。サプライヤーは、シティの独自の裁量により、懸念に対し納得できる形で対処するため、迅速に必要な修正措置を取る、および/または必要な救済措置を追加する必要があります。この対処に必要な期間は、高リスク問題の場合は 180 暦日以内、中程度のリスクの問題では 240 暦日以内、低リスクの問題ではシティがリスク評価を行うため、次のコンプライアンス期日までと定められており、遵守しなければなりません。

1. サプライヤーはその独自の情報セキュリティ基準、ポリシー、手順に照らし合わせて、ビジネス業務と関連規制事項を定期的に評価しなくてはなりません。定期的な評価には少なくとも以下を含めなければなりません。
 - a) サプライヤーがサプライヤー独自の IS ポリシーと基準の遵守を徹底するために使用するプロセスの評価
 - b) サプライヤーが使用するアプリケーションおよびインフラストラクチャ、ならびにサプライヤーの業務委託先がそれらの業務活動をサポートするために、またはシティがこれらの評価を行うために使用する IS プロセス（該当する場合）などの補助リソースの評価。第三者が、シティが「機密」またはそれ以上のカテゴリに分類したシティ情報へのアクセス、処理、管理、または廃棄を行う再委託業者と新規契約を締結する際、または既存の契約を更新する場合にもコンプライアンスが求められます。
2. 情報セキュリティリスク評価（TPISA など）によって特定された問題は文書化し、終了するまで追跡し、是正された証拠をシティに提示しなければなりません。
3. サプライヤーの情報セキュリティ管理部門が国外に移転される場合、サプライヤーはその移転前にシティの承認書を取得する必要があります。

4. サプライヤーが新しい組織を買収した場合、サプライヤーはこれらの要件の遵守について買収した組織の査定を行わなくてはなりません。
5. サプライヤーは、シティが事前に書面で承認しない限り、セキュリティ管理機能を外注することはできません。この中には、シティ情報の保管、処理および/または送信に使われるシステムのファイアウォール管理、セキュリティ設定管理、パッチ管理、または情報セキュリティ管理(ISA)機能が含まれますが、これらに限られません。
6. サプライヤーが、ソフトウェア、またはシティ情報が含まれているウェブサイト、あるいはシティブランドのウェブサイトのホスティングを行う場合は、シティのシステムセキュリティテスト基準(SSTS)に従って定期的な脆弱性評価を行い、評価中に特定された重大な問題をその基準に指定される期間内に修正する必要があります。SSTS は外部への配布が承認されていないため、サプライヤーはシティ・リレーションシップ・マネージャーと協力し、必ず参照文書を遵守する必要があります。さらに、サプライヤーは、関連する ISO/IEC 27001 情報セキュリティ管理基準（または、より高い基準やプロトコルを定めた後継の情報セキュリティ管理基準）、および本セクション（17）にある情報セキュリティ規定を遵守します。
7. サーバーおよび/またはシティ内部ネットワーク上の情報システムに接続する必要がある場合、サプライヤーは現在の接続プロビジョニングプロセスを遵守できるよう、シティの主要連絡窓口へ通知する必要があります。
8. サプライヤーは、シティの情報に対する不正なアクセス、取得、損失、不正操作、削除、およびシティの情報の保管、処理および/または送信に使われる情報システムへのその他の不正アクセスについて、適切なシティの連絡窓口（ビジネス活動担当責任者：BAO）に速やかに通知する必要があります。
9. サプライヤーは、すべてのハイリスクな行動または機密データの変更について、どの人物がどの活動を行ったかを特定できる監査証跡が残されていることを確認する必要があるとあります。
10. サプライヤーは、画面上および書面上の分類が機密またはそれ以上のデータを見えないようにカバーする必要があります（監視、例外、および規制、およびその他のレポートを含む）。
11. サプライヤーは、「個人所有の機器類」も含め、機密データの印刷、記録、または複写を制限しなければなりません。サプライヤーは、法律または規制で禁

止されていない限り、契約期間中の合意された時点で、または契約終了時にシティの情報をすべて返却または破棄するものとします。

12. サプライヤーは、シティの情報にアクセスするサプライヤーの全人員（従業員、業務委託先、臨時従業員、業務委託先）が、秘密保持契約書または守秘義務契約書に署名していることを確認する必要があります。
13. サプライヤーの従業員には、サプライヤーの行動規範および人事ポリシーの違反や不履行に対する懲戒プロセスが記載された従業員ハンドブックまたはそれと類似する文書を提供し、従業員はこれを入社プロセスの一環として受け入れなければなりません。
14. サプライヤーは、従業員または非従業員が解雇された、または退職したときにすべての資産を回収するプロセスを備えています。
15. 機密情報がウェブサイトまたはウェブでアクセス可能なシステム上に保持または保存される場合、サプライヤーはシティにこの情報を開示しなければなりません。この開示は本サービスの説明に含まれる場合があります。サプライヤーがシティの機密情報を保持または保管する場合、サプライヤーは本書期間中、年に一度、SSAE 18 監査（または、シティが承認する、後継の権威ある評価）を実施させ、当該 SSAE 18 監査またはシティが承認する、後継の権威ある評価の結果を文書化した報告書の写しを、年に一度以上、シティに提供するものとします。
16. サプライヤーが合併、買収または類似の取引において他の事業体を買収し、当該取引が本サービスに影響を与える可能性がある場合、サプライヤーは速やかにシティに書面で通知しなければならず、サプライヤーは、買収や合併が本要件の遵守に影響しないことを確認するため、合併、買収等の結果として生まれる事業体について本要件と整合する情報セキュリティ評価を実施しなければならないものとします。

17.5 再委託業者の情報セキュリティリスク

サプライヤーは、シティの、分類が機密またはそれ以上のデータにアクセスする業務委託先に対し、資格のある情報セキュリティ担当が行う契約締結前および定期的な契約後の情報セキュリティ（IS）評価を義務付けなければなりません。これらの評価は、開始から問題管理までの評価プロセスのすべての段階に対処する、経営陣が承認したプロセスに従って行う必要があります。業務委託先の IS 評価は、シティの第三者 IS 評価アンケート（TPAQ）に含まれるものと一致する IS 領域内の業務委託先の姿勢

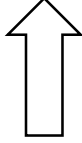
を評価するアンケートまたは同等のツールを活用すべきであり、業務委託先の関与に関連する IS リスクを算出する論理的方法を含める必要があります。サプライヤーは評価完了を追跡し、指摘された問題と是正措置計画を管理して終了する必要があります。

17.6 資産に対する責任

1. サプライヤーは、シティ情報の保管、処理、送信に使われるアプリケーションとハードウェアがすべてインベントリで管理されていることを確認する必要があります。
2. サプライヤーは、シティ情報資産インベントリが、かかるインベントリの正確性および完全性を適切に維持するために使用される手順に従って管理維持されていることを徹底しなくてはなりません。
3. サプライヤーは、その管理下にあるシティの情報をすべて保護する責任を負わなければなりません。
4. サプライヤーは、業界の慣行と一致する方法でユーザーの活動の説明責任を確保する必要があります。
5. シティ情報が存在するサプライヤーのグローバルネットワークから個人的な外部インターネットの E メールストレージとクラウドストレージのアカウントへのアクセスは制限しなくてはなりません。

17.7 情報分類と取扱い

シティは下表の情報分類に基づいて情報を分類します。以下の各情報分類の定義および例については、付録をご参照ください。

極秘	最も機密性が 高い
機密性が高い PII	
機密 PII	
機密	
社外秘 PII	
社外秘	
一般公開	最も機密性が 低い

1. シティ情報の分類に基づき、シティはサプライヤーと協力して当該情報の保護に必要なセキュリティのレベルを特定します。またサプライヤーは、こうしたセキュリティレベルにおける十分な管理の設定を徹底しなくてはなりません。このレベルはシティにより引き上げられたり修正されたりする場合があります。
2. 社外秘またはそれ以上に分類される情報は、シティのポリシーおよび基準に従った機密条項を含む、シティと第三者との間に締結された契約の対象となる第三者が管理する機器に保管されなければなりません。
3. サプライヤーがシティデータの保存にサプライヤーが所有しない機器（すなわち、第四者が管理する機器）の使用を許可する場合、サプライヤーは特定の経営陣による承認を義務付けるポリシーを設定し、シティの情報の使用と破棄に関するガイドラインと監視手順を定めなければなりません。
4. サプライヤーは常に、不正なアクセスや改ざん、削除からシティの情報を保護しなければなりません。
5. 電子輸送可能メディア(ETM)を介して転送される機密またはそれ以上に分類されるシティ情報は、承認された暗号アルゴリズムを使用して暗号化され、受領を確認する必要があります。サプライヤーは、ETM が意図された方法で受領されたことを確認しなければなりません。受領予定日に受領を確認できなかった場合、サプライヤーはシティに通知する必要があります。

17.8 安全設定

1. サプライヤーには、シティの情報を保存、処理、アクセス、または送信する可能性のあるすべての資産について、文書化された安全設定基準を維持することが義務付けられます。

2. サプライヤーは、アプリケーション、商品、サービスの選択、開発、実装のプロセスと手順に情報セキュリティコントロールを取り入れる必要があります。
3. サプライヤーは、シティの情報が保存、処理、送信されるシステムすべてについて安全な構築手順を設定するものとします。
4. サプライヤーはすべてのシステムの安全なイメージまたはテンプレートを維持する必要があります。
5. デフォルトのユーザーアカウントとパスワードはすべて、ベンダーがサポートするシステム、ネットワークデバイス、およびアプリケーションから削除および/または変更しなければなりません。
6. 侵害されたシステムやサービスは、完全性が実証されたイメージやテンプレートを使って再構築し、設定しなければなりません。
7. 安全な設定の変更はすべて、サプライヤーの変更管理プロセスを通じて経営陣が承認しなければなりません。
8. 安全な設定に変更があった場合、サプライヤーはシティに通知しなければなりません。
9. 安全な構築手順には、実稼働デプロイメント時におけるセキュリティ/標準構築設定の自動設定確認をサポートするツール、および、基本構成への準拠と基本構成からの逸脱を継続的にモニタリングするツールが含まれていなければなりません。

17.9 暗号化要件

サプライヤーは、暗号化されていない、機密またはそれ以上の分類情報を送信してはなりません。機密またはそれ以上に分類される情報は、シティが承認したツールまたはソリューションにより**エンドツーエンド**で暗号化されなければなりません。暗号化されたデータ送信について承認されたプロトコルと各バージョン番号は以下の通りです。

1. 認証および認証情報を交換する場合：SAML v2.0、OAuth v2.0（認証のみ）
2. 通信チャネルおよび関連するキーの交換を保護するために、以下のネットワーク・セキュリティー・プロトコルのみが許可されている場合
 - a) TLS v1.3 が優先され、すべての TLS v1.3 スイートが許可されます。
TLS v1.3 が有効なプロトコルのみである場合、追加レビューは不要です。

- b) TLS v1.3 が技術的に実行可能ではなく、TLS 1.2 が活用されている場合、現在は SSLabs の B 以上のグレードが許容され、追加レビューは不要です。

シティの第三者環境に永続的に保存されるデータまたは交換されるデータは、シティが承認したツールまたはソリューションを用いて完全に暗号化されなければなりません。データを暗号化するために承認されているアルゴリズムとキーの長さは以下の通りです。

1. **高度暗号化基準（AES）**：承認されたキーの長さ：256 ビット以上。制限付きモード：電子コードブック（ECB）モードは、平文の量がブロック長以下の場合を除き、禁止されています。ディスクドライブの暗号化：256 ビットキーの AES が必要です。キーの長さが 128 ビットの AES は TLS 暗号オプションとして認められていますが、シティが国際的なスケジュール（参照、NIST 8547 IPD）に合わせて、2028 年 12 月 31 日までに 256 ビット以上のビット強度へと移行するため、使用が禁じられます。
2. **ChaCha20（関連するユースケースのためのストリーム暗号）**：承認されたキーの長さ：128 ビットまたは 256 ビット、96 ビットナンスと 32 ビットブロックカウントまたは 64 ビットナンスと 64 ビットブロックカウント。最大データサイズ：16 ペタバイト

承認された公開キー暗号システム、キー交換、合意メカニズム、メッセージダイジェスト、およびキー導出関数は次のとおりです。

サプライヤーの量子レディネスに関する通知：サプライヤーは、NIST IR 8547 (ipd) の表 2 と表 4 をカバーする計画をシティ量子レディネスプログラムチーム ([survey link](#)) に提示する必要があります。

1. **公開キー暗号システムと最小キー長サイズ**
 - a) Rivest-Shamir-Adleman (RSA)：2048 ビット
 - b) Digital Signature Algorithm (DSA)：2048 ビット DSA は、シティの外部で処理または保存されたシティのデータをセキュリティ保護する目的で使用してはなりません。
 - c) Elliptic Curve Digital Signature Algorithm (ECDSA)：256 ビットで、ANSI X9.62 に規定されている NIST 推奨曲線に従います。
2. **キー交換および合意メカニズムと最小キー長サイズ**

- a) ディフィー・ヘルマン (DH) / 一時的なディフィー・ヘルマン (DHE) 2048 ビット
 - b) Elliptic-curve Diffie–Hellman (ECDH) / Ephemeral Elliptic-curve Diffie–Hellman (ECDHE) : 256 ビットで、ANSI X9.63 に規定されている NIST 推奨曲線¹に従います。
3. **メッセージダイジェスト機能**：ハッシュを生成するために使用される素材に含まれるランダムビットの数よりも大きな長さの暗号化キーを作成することは禁止されています。
- a) SHA-1 デジタル署名以外の用途にのみ使用可能です。SHA-2 ファミリー、SHA-3 ファミリー、POLY-1305：すべての暗号化ハッシュ関数アプリケーションで使用可能です。
4. **パスワードによるキーの導出関数と最小要件**
- a) PBKDF2：最低反復回数は 10000 回、ソルトは最低 16 バイト。
 - b) HKDF：ソルト化する必要があり、情報入力値を含める必要があります。
 - c) SCRYPT：最小ラウンド数/コスト係数 10。
 - d) ストリーム暗号化に NIST SP800-108 KDF を使用することは禁止されています。NIST SP 800-108 KDF モード、すなわちカウンター、フィードバックおよび二重パイプラインイテレーションモードが許容されます。
 - e) Argon2 を推奨します。
5. **パスワードハッシュ関数と最低要件**
- a) Bcrypt（認証マテリアルのローカル保存用）：最小ラウンド数/コスト係数 10 以上。
 - b) Argon2 または PBKDF2 は、サプライヤーの製品で展開された環境またはシステムにパスワードをローカルに保管する場合、パスワードハッシュに推奨されます。

17.10 社外 E メール

規制および/またはサプライヤーのポリシーにより、シティによって承認済みのエンドツーエンド暗号化ソフトウェアまたはツールの使用がサプライヤーに許可されない場

¹ECDHE が優先されます。

合、シティ情報分類が「機密」以上に該当するシティの情報が含まれる個人の電子メールをシティとサプライヤー間でやり取りする際の暗号化要件は、転送の暗号化（トランスポート層セキュリティ(TLS)によるゲートウェイ間の暗号化など）を通じて完全に満たすことができます。承認された安全な E メールプロトコルは次のとおりです。

1. **Identify-Based Encryption (IBE)** の特徴は暗号化 E メールで、シティ内の顧客対応ソリューションと安全な E メール、および eDelivery システムに使用することができます。
2. **Mandatory TLS (MTLS)** の特徴は、セッション暗号化（E メールペイロードは暗号化しない）で、その使用について事前に交渉を行っているベンダー、パートナーおよびクライアントに使用することができます。
3. **Domain Keys Identified Mail (DKIM)** の特徴はソース認証と鍵管理で、ベンダー、パートナー、およびクライアントに使用することができます。

17.11 プライベートネットワーク

認定機関が独立して規制し、ライセンスがあるか認定を受けている相手（SWIFT または中央銀行など）とのビジネス取引に対する金融サービス業界基準を満たすプライベートネットワークは、これらのネットワークが暗号化された送信を完全にサポートするために必要なインフラストラクチャを提供するまでは、機密 PII の送信中の暗号化要件の対象外とみなされる場合があります。

17.12 音声およびファックス

シティの分類で「機密」以上の情報をファックスで送るか、これについて電話（ボイスオーバーIP [VOIP]など）で話し合う場合は、暗号化しなくても構いません。必要な場合、サプライヤーはこのような方法で送られる機密以上の情報を保護するための具体的な手順と指針を策定しなければなりません。

17.13 暗号鍵と証明書の管理

このセクションで使用されるセキュアな境界という用語は、連邦情報処理規格（FIPS）、検証された境界（最低許容されるセキュリティレベルは FIPS 140-2/3 レベル 2）などの暗号モジュール認証制度（CMVP）を指します。（AWS Nitro Enclaves などの機密コンピューティングエンクレーブは使用可能です。その他のユニークなセキュリティ境界の案件は、シティの承認を受ける必要があります。）

1. サプライヤーは、（SSH キーを含む）最新の業界基準の暗号化アルゴリズムを実装し、暗号化と署名には最低の鍵長を設定しなければなりません

。サプライヤーは、そのようなアルゴリズムと鍵長が業界標準と整合するよう更新された場合、変更管理プロセスを通じて保証を提供しなければなりません。

2. サプライヤーは、機密性の高いマテリアルを不正使用または漏洩から保護するための管理体制を備えた、正式に文書化されたキー、秘密、証明書管理ライフサイクルプロセスを持っていなければなりません。すべての暗号化秘密と鍵のライフサイクルイベントは、セキュアな境界内でしか発生させることはできません。特権のあるセキュアな境界へのすべてのアクセスは、すべて文書化されなければなりません。サプライヤーは、関係するアクター、エンティティ、および境界を強調した、すべての主要なライフサイクルイベントのシーケンス図を提供しなければなりません。
3. 暗号化キーには固有の目的が必要であり、他社のデータの暗号化や第三者の内部使用など、他の目的に使用してはなりません。例えば、ディスク暗号化とデータ暗号化に同じ暗号化キーを使ったり、ペイロード暗号化とデータベース暗号化に同じ暗号化キーを使ったりしてはなりません。**SaaS** サプライヤーによる複数のテナント間の暗号化キーの再利用はデフォルトでは禁止されており、セキュリティ・アーキテクチャ・カウンシルの明示的な承認を得て、機密 **PII**、極秘 **PII**、および制限付きに分類されるシティ情報を含む重要ではない、リスクの低い使用案件にのみ許可される可能性があります。
4. すべての暗号化キー（対称または非対称）について、秘密キーまたは秘密キーマテリアル（シードや秘密キーの一部など）は、いかなる場合も平文で表示してはなりません。秘密キーまたは秘密キーマテリアル（シード、または秘密キーの一部など）は、動的なセッションキーなどの一時的なキーを除いて、セキュアな境界を離れることは絶対にできません。設計上、セキュアなエンクレーブ/特権アクセス境界間で対称キー、秘密キーまたは秘密キーマテリアルの導出が必要とされる場合、相互 **TLS** 暗号化トンネルを介してのみ、対称キーラッピングキーまたは公開キー転送キーを使用して暗号化された形式で送信され、そのような送信はシティが書面で承認する必要があります。秘密キー 転送キーは、このような場合、生成された特権アクセスセキュアな境界を離れることは絶対にできません。
5. 対称キーラッピングキーは、2 つ以上のキーコンポーネントに分割し、配布前および手動のキー入力/読み込みのために **XOR** する必要があります。対称

キーラッピングキーは、**CMVP** 検証済みモジュールなど、セキュアな境界内部で適切なアクセス・コントロール・リスト（**ACL**）を持つ必要があり、対称キーラッピングキーはセキュアな境界外に保管することはできません。

6. 秘密キー、秘密情報、秘密キーマテリアル（シード、秘密キーの一部など）を含むキーストアまたはセキュアな境界への人間またはサービスもしくは自動エージェントによるアクセスは、許可された個人またはシステムのみへのアクセスを制限するコントロールを使用して適切に分離する必要があります。
7. 秘密キーまたは対称キーを含むキーストアにアクセスするためのすべての要求は、監査目的で、誰が、いつ、何の目的でアクセスしたかなどの詳細とともにログに記録し、文書化する必要があります。
8. サプライヤーは、自己署名証明書、ワイルドカード証明書、またはデフォルトの **SSL** 証明書を使用してはなりません。
9. すべての暗号化キーには、**NIST SP800-57 part 1, revision 6** で提案されているように、暗号化期間のタイムスパンを定義する必要があります。キーは、有効期限前に更新またはローテーションして、変更、スケジュールの重なり、システムフリーズの期間を調整しなければなりません。
 - a) 期限が切れた証明書を交換する際、古い非対称キーペアを再使用することは禁止されています。
10. 暗号化キーは、キーの完全性、キーが保存または共有されるメディア、または対称キーまたは秘密キーが漏洩すると疑われる時点で、侵害されたものとして扱わなければなりません。侵害されたキーはすべて業務上の使用から削除され、対応するすべての証明書を失効させる必要があります。
11. ワイヤレスネットワークは、業界標準の暗号化アルゴリズムで暗号化するものとします。
12. あらゆる形態の暗号化メカニズムを活用するサプライヤーは、業界標準のキー管理ツールとテクニックを使用するものとします。主な管理役割は、業務管理から分離されなければなりません。
13. サプライヤーは、シティのデータセキュリティサービスにより提供される **PKI & KMS** サービスとの相互運用性が保証され、シティの暗号化ガバナンス外で暗号化制御が委任されていない場合にのみ、クラウドベースの **KMS** および **PKI** を活用することができます。

17.14 アクセス制御の責任

シティの機密またはそれ以上の情報の保存/アクセス/管理/処理/送信に使用される規制情報システムのすべてを不正アクセスから保護するため、サプライヤーは、各業務機能に必要な最低レベルのアクセスにユーザー権限を制限し、すべてのシステムとアプリケーションへの論理的アクセスの提供を管理することにより、最小特権の原則を実施する責任を負います。制御は完全に文書化され、監査可能でなければなりません。パスワードのリセットや有効化を含むアクセス権の付与および解除は、権限の過剰付与による潜在的な人為的ミスリスクを軽減し、業界標準に準拠するため、可能な限り自動化されたプロセスを通じて実施する必要があります。

1. サプライヤーは、自らの組織内の全ユーザーのアクセス権について責任を負います。
2. サプライヤーはアクセス制御を実施し、ユーザーが職務の遂行に厳密に必要な特権と資格のみが付与されるよう徹底する必要があります。
3. サプライヤーは、不正な使用を防ぐため、すべてのデフォルトのアクセス能力が削除、無効化、または保護されるようプロセスを実装しなければなりません。

17.15 ユーザーアクセス管理

サプライヤーは、シティの機密またはそれ以上の情報を処理、保存、および/または送信するシステムとアプリケーションへの論理的アクセスの提供を管理するものとします。これには次の事柄が含まれます。

1. 承認された認証システムの識別とインベントリ。
2. マネージャーまたはマネージャーの被指定人とシステムオーナーの承認が義務付けられるシティデータへのすべてのアクセスの要件。サプライヤーは、シティのデータにアクセスできる従業員が、知る必要がある場合にのみアクセスできるようにする責任を負います。
3. 利益相反またはメーカーチェッカー規則の違反となる場合、個々のユーザーに対する特権/機能のいかなる組み合わせも提供することができないという要件。
4. システム上の各ユーザーに付与された/取り消されたアクセス権を監督し、管理するモニタリングプロセス。

5. アクセス権限の申請は、他のユーザーの権限をミラーリングまたは複製することに依拠してはなりません。権限の拡大を防止し、最小権限の原則を徹底するため、申請には業務上の根拠を明記した上で、具体的な役割および権限を明示する必要があります。

17.16 ユーザーID および認証

サプライヤーが管理する情報システムはすべて、シティの情報にアクセスできるセッションや取引を開始する前にプラットフォームにアクセスするユーザーまたはシステムの ID を認証するものとします。

1. ユーザーは、ユーザーID によって一意に特定されるか、技術プラットフォームにマッピングできなくてはなりません。
2. ユーザーは、承認された認証方法を使用して技術プラットフォームに認証されなくてはなりません。承認されている最新の方法については、主要連絡窓口（BAO）に問い合わせてください。
3. 共有認証インフラストラクチャ（シングルサインオン、リデュースドサインオン、その他の共有認証サービスなど）を使用する場合は常に、シティの認証要件に従う必要があります。承認されている最新の方法については、主要 BAO に問い合わせてください。
4. 情報システムに対するユーザーの認証に使用される ID 検証データ（IVD）は、伝送および保存において暗号化されなければなりません。暗号化要件についてはセクション 17.9 を参照してください。
5. サプライヤーの担当者がシティのシステムにアクセスするために使用するすべてのアカウントは、シティが割り当てた一意の識別子（例：GEID）に紐付けられていなければなりません。追跡可能性の確保、職務分掌（SOD）の徹底、および監査対応を確実にするため、人間ユーザーによる汎用／共有ユーザーID の使用は禁止されています。

17.17 特権アクセスの特定および一時的な特権アクセス

サプライヤーは、すべての ID のインベントリを維持し、機密 PII またはそれ以上に分類される情報を含むアクセス特権があるもの、または電子リポジトリ（ビジネスアプリケーションをサポートするデータセットまたはデータベース）にアクセスできるものを特定する必要があります。サプライヤーは、これらの ID の不正使用から保護する

コントロールを実装するものとします。労働者が特権 ID や前述の電子的リポジトリへのアクセスを必要とする場合、そのアクセスは、以下に該当する一時的なアクセス管理プロセスを通じて付与されなければなりません。

1. 申請者は事前に承認された認定ユーザーリストに含まれているか、使用時に承認を確保することを義務付ける。
2. アクセスを付与する前に、変更/問題チケットで正当な理由を文書化することを義務付ける。
3. アクセス権を使用して行われた活動の独立したレビューが含まれている。
4. 一時的なアクセスリリース期間の終了時にアクセスの取り消し/削除を開始するためのプロセスが含まれます。
5. 稼動および実装後の安定化アクセス（主要なアップグレードやブレイク/フィックスの解決後など）には、最高で7暦日のアクセス権延長を許可する。

17.18 ユーザーアクセス権のレビュー

1. サプライヤーは、シティ情報の保存、処理、管理、および/または送信に使われる規制情報システムに対して不要なユーザー資格がないかを年2回以上見直して確認し、削除するプロセスを文書化して実施する必要があります。
2. ユーザーは、自分自身の資格、またはレビューを任されている個人の資格をレビューまたは承認することはできません。
3. シティのサプライヤー従業員の職務変更後、サプライヤーは、14 暦日以内にアクセスおよび特権審査を行い従業員の新しい職務に必要とされない場合はシティデータへのアクセスを削除します。

17.19 安全なログオン手順

1. ロックアウトされたユーザーのログイン ID は、業界基準のリセットサービスまたは別の認定機能によって再度有効にしなければなりません。バナーテキストは、オペレーティングシステムまたはアプリケーションがサポートしている場合、ユーザーのサインインまたは認証が行われるすべてのネットワークのエントリポイントで表示される必要があります。

17.20 パスワード管理システム

1. ユーザーの静的パスワードは決して画面上に平文で表示してはなりません。パスワードの表示・非表示を切り替える機能については、以下の条件を満たす場合に限り、この要件の適用除外となります。
 - (1) パスワードの入力は、デフォルトでマスク表示されている
 - (2) パスワードの表示は、ユーザーによる明示的な操作によってのみ開始される。
 - (3) ユーザーの操作が中断されてから最大 15 秒以内に、パスワードは自動的に再びマスクされる。
2. 特権のある機能 ID のパスワードは平文でハードコード化してはなりません。
3. 静的パスワードは 10 字以上で、文字と数字の双方を含める必要があり、大文字と小文字を区別できるようにします。静的パスワードの大文字・小文字の区別については、各認証ポイントで検証を行う必要があります。2026 年 8 月 31 日以降に導入されるアプリケーションにおいて、職務 ID (FID) の静的パスワードは、15 文字以上でなければなりません。
4. PIN は、物理的なデバイスの制約（キーパッド、電話、スマートカードなど）に従うために PIN が必要な場合にのみ情報システムにアクセスする唯一の認証方法として使用できます。
5. 静的なパスワードはすべて、最低でも 90 暦日ごとに変更する必要があります。
6. 静的なパスワードはすべて、ログイン試行が最高で 6 回連続して失敗した後、またはパスワードのリセットが 6 回連続で試行された場合、ロックアウトされる必要があります。パスワードは ID 管理者機能を使ってロック解除するか、少なくとも 30 分後に自動的にロック解除される必要があります。
7. 認証システムはすべて、100 暦日を超えないログイン非活動/非使用制御を実行する必要があります。技術的に可能な場合、無効なログインは、ユーザーまたは別の認定職務によって再度有効にすることができます。
8. 認証プロセスでは、同じパスワードが少なくとも過去 6 回の変更で使用されていないことを確実にする必要があります。

17.21 システムユーティリティの使用

サプライヤーは、システムおよびアプリケーションのコントロール機能をオーバーライドできるユーティリティプログラムの使用が制限され、管理されていることを徹底する必要があります（周辺機器からの起動など）。

17.22 セッションタイムアウト

1. シティの情報の保存、処理、送信で使われる規制情報システムの全ユーザーについて、ログインまたは再認証が必要になります。
2. 非アクティブ時間が 30 分以内に再認証するよう、ユーザーに求める必要があります。アクティビティには、エンドポイントへのあらゆる入力（マウス、キーボード、タッチスクリーンなど）が含まれます。パスワードで保護されたスクリーンセーバーを使用している場合は、アプリケーション/シングルサインオンは不要です。

17.23 ユーザーアクセスの終了

1. 解雇または退職した時点で、シティの機密またはそれ以上のデータへのアクセスを許可することができるユーザーアクセスまたは特権（デスクトップ / アクティブディレクトリへのユーザーログイン、シングルサインオン [SSO]、E メール、1 回限りのパスワード（OTP）トークンおよびリモートアクセスユーザーログイン）は、直ちに削除するものとします。
2. 従業員にシティが所有および管理するシステムへのアクセス権がある場合は、シティのビジネスリレーションシップマネージャー、BAO、または BAO サポートを、その従業員の職務が変更または終了した時点で速やかにシティに通知し、シティのビジネスマネージャーが解雇日の終わりまでに、解雇された従業員のアクセス権の削除を開始できるようにします。
3. サプライヤーは、従業員または非従業員が解雇された、または退職したときに、セクション 17.23.2 に定められた時間枠に沿って、すべての資産からアクセスを回収するための文書化されたプロセスを設定します。
4. 17.23.1～17.23.3 に関してサプライヤーが何らかの異常を発見した場合、サプライヤーは適切な根拠とコントロールを提示しながら、直ちにシティのビジネスリレーションシップマネージャー、BAO、または BAO のサポートに報告するものとします。

17.24 リモートアクセス

サプライヤーには、以下を含むシティの機密またはそれ以上のデータを保存、処理、または送信できるネットワークへのアクセスを保護するためのリモートアクセス制御がなければなりません。

1. シティの情報の保存、処理、管理、または送信で使われる情報システムへのリモートアクセスは、不正使用から保護されなければなりません。
2. シティの情報分類が機密またはそれ以上である情報のローカルストレージ/処理が行われる場所へのリモートアクセスを使用して、シティの情報の保存、処理および/または送信に使われるサプライヤーが管理しているすべてのノートパソコンとすべてのサプライヤーが管理しているデスクトップは、業界基準を満たす暗号化ツールを利用して暗号化する必要があります。
3. リモート接続は、多要素認証（MFA）を採用した承認済みのリモートアクセスソリューションを通じてのみ確立することができます。
4. サプライヤーが管理しているコンピュータを直接インターネットに接続する場合は、個人のファイアウォールを有効にしなければなりません（つまり、サプライヤーが管理するファイアウォールまたはプロキシを介さないこと）。
5. サプライヤーが管理する機器は、ネットワークへの完全なアクセスの要件として定期的なソフトウェア/ウイルス防止ツールのアップデートを受信およびインストールするため、サプライヤーのネットワークに定期的に接続される必要があります。デバイスの更新を明確な目的とする場合は限定的なアクセスが許可されます。
6. シティの機密またはそれ以上の情報にアクセスするためにサプライヤーが所有および管理しないデバイスを使用する場合、そのデバイスには、ローカルマシンへのダウンロードを許可しないようにする認可済みのソリューションを使用するよう設定しなければなりません。以下のような制御対策を実装しなければなりません。
 - a) 会社が管理するソリューションを使用しないデバイスにシティのデータがダウンロードされないようにする。
 - b) アクセスが標準的なリモートアクセス技術（仮想デスクトップインターフェース：VDI など）を使用し、トークンまたは証明書のいずれかに基づく認証によって保護されていることをサプライヤーは徹底するものとします。
 - c) **Terminal Services**、**VMware Horizon** などのリモートアクセスソリューションは、クリップボード共有、**Drive Mapping over Blast**、**PCoIP**、**RDP** プロトコルと **SSH** プロトコルを無効に設定しなければなりません。

7. モバイルデバイス上のソフトウェアアプリケーションにアクセスするなど、ソフトトークンを **MFA** に使用する場合、ソフトトークン認証ソフトウェアは、（パスワード、生体認証などで）ユーザーを認証し、携帯電話がジェイルブレイクまたはルート化（モバイルデバイスベンダーによって認証・供給されていない **OS** を使用）された場合は使用を阻止するものとします。
8. システム管理者、データベース管理者、アクセス制御管理者、ファイアウォール管理者、ウェブサイト管理者など、シティに提供するサービスに直接的または間接的に関連するシステム、データリポジトリ、アプリケーションおよびインフラへの特別、特権的、または管理レベルのアクセスを要する正社員、契約社員および業務委託先を含むがこれに限らない全てのサプライヤーの人員は、**MFA** のみを経由して認証し、当該アクセスはこれらの要件に従い、疑わしい活動および/または不正なアクセスをサプライヤーが独自に記録及び監視するものとします。
9. 個人所有のデバイスおよび第三者が所有するデバイスについて、サプライヤーは、そのようなデバイスがネットワークにログオンすることを許可される前に、そのデバイスが承認されたオペレーティングシステムのバージョン、パッチレベル、ウイルス防止、マルウェア防止ソリューションを有していることを確認するための効果的なソリューションを有していなければなりません。
10. サプライヤーは、すべての従業員が以下を実行していることを確認するものとします。
 - a) 音声アシスタントデバイス（**Siri**、**Alexa** など）、ビデオ録画機器、その他の写真、ビデオ、音声のリスニング/録音機器を一切使用しないプライベートな専用のリモートワークスペースを維持すること。権限のない者が、リモートコンピューティングシステムの画面に表示されるデータ、システム、アプリケーションを閲覧することを許可されないこと。
 - b) デバイスを無人で放置する場合は、コンピューティングデバイスをロックし、画面を表示するための不正アクセスが適切に防止されるようにすること。

17.25 クリアデスク ポリシー

サプライヤーのスタッフは、あらゆる形態のシティの情報（ワークスペースで使用または保管される物理的な情報など）を保護する必要があります。サプライヤーはこの要件について、少なくとも年に 1 度、IS トレーニングやその他の手段を通じてサプライヤーの全スタッフに連絡する必要があります。

17.26 防火

1. サプライヤーは、物理的なセキュリティと（現地の消防法など）安全な労働環境の構築に関する適用法令の要件に従う必要があります。
2. サプライヤーは火災検知、警報、防火システムを利用するものとします。このようなシステムは年 2 回点検し、年 1 回テストしなければなりません。

17.27 物理的セキュリティ

1. シティの情報は安全なエリアに保存され、権限のある従業員のみにアクセスを制限するよう管理する必要があります。
2. サプライヤーは、文書化され、監査可能な物理的なアクセス制御システムを設置する必要があります。
3. サプライヤーは、提供される環境とサービスに応じて、サードパーティ、警備員が監視するセキュリティアラーム、警備員、ビデオ監視を含むセキュリティアラーム/侵入システムを組み合わせる必要があります。
4. サプライヤーは、訪問者に関するポリシーを文書化しておく必要があります。この中には、すべての訪問者の到着時に確認可能な ID を提供し、入退室を記入する要件が含まれます。

17.28 業務上のセキュリティ手順と責任

1. サプライヤー変更管理プロセスには、変更登録、レビュー、テスト、承認、実施、および終了に関する主要なチェックポイントコントロールを含める必要があります。サプライヤーにはまた、義務付けられている承認の階層を含む、記載されたすべての段階を必要とする緊急変更プロセスを保持していなければなりません。
2. サプライヤーは、キャパシティ管理に関する監査可能なプロセスを備えていなければなりません。これには可用性、キャパシティ、パフォーマンスメトリクス/指標、ビジネスへの影響評価、パフォーマンスとキャパシティ

に関する問題に対する積極的な追跡、調査、対処が含まれますが、これらに限定されません。

3. 適宜、サプライヤーはラボ、開発、テスト、実稼働環境がすべて物理的および/または論理的にお互い分離されていることを徹底する必要があります

17.29 ソフトウェア開発要件

適用対象はシティの単独使用を目的として開発されたソフトウェアを提供するサプライヤーです。サプライヤーは、これらの要件を遵守するか、あるいは同等の品質を確保するアプローチを採用した、文書化され承認済みのソフトウェア開発ライフサイクル（「SDLC」）プロセスを提示しなければなりません。

17.30 着手と計画

サプライヤーは、シティの要件および契約上の義務に沿って、ソリューションの範囲と目的を定義しなければなりません。これには次の事柄が含まれます。

1. 機能的および非機能的要件を文書化すること
2. 工数およびスケジュールの見積もりを提示すること、かつ
3. すべてのサードパーティ製コンポーネントまたは依存関係を特定すること

セキュリティリスク評価を含むコンプライアンスアクティビティは、プロジェクト開始時に開始する必要があります。役割、責任、および承認のチェックポイントは、明確に伝達されなければなりません。

すべての環境は、「開発（DEV）」、「テスト（TEST）」、または「本番（PROD）」のいずれかに分類され、ライフサイクル全体を通じて厳格に分離されなければなりません。環境の分類によってアクセス権限や処理可能なデータの種類の種類が決まります。サプライヤーは、環境の指定に基づいてアクセスを制限し、展開を適切な SDLC フェーズの完了状況に合わせて行うことで、不正アクセスやデータ漏洩を防止しなければなりません。

17.31 設計

サプライヤーは、納品されたソリューションが記載されたすべての要件（以下「テスト計画」といいます）を満たせるよう、設計アプローチを文書化する必要があります。テスト計画書には、少なくとも以下の項目を含め、その内容を記述する必要があります。

1. 1.開発チームが実行するすべてのテスト（ユニットテスト、機能テスト、非機能テスト、およびパフォーマンス関連のテストを含む）は、要件へのトレーサビリティを確保すること
2. 2.完了を確認する承認者の特定
3. 3.脆弱性評価や脅威モデリングなどのセキュリティテスト要件
4. 4.テスト環境、アプローチ、プロセス、および昇進の道筋。

リリース戦略を策定し、プロジェクト期間を通じて、TEST 環境および PROD 環境へのリリースに必要な前提条件とプロセスを明記する必要があります。これには、リリースの準備完了基準、リリース内容、およびリリース頻度を含める必要があります。

契約書に明記されている場合、ソフトウェアの配布物は、シティが承認したツールおよびワークフローを用いて、シティが承認した形式でパッケージ化されなければなりません。

17.32 テスト

ソリューションが定義された要件および成功基準を満たしていることを検証するためには、テストを計画し、管理された環境下で実施する必要があります。テスト案件は要件およびコードのコミットに、トレーサビリティが確保されていなければなりません。

サプライヤーは、合格・不合格の結果、開発中に実施された追加試験、および未完了の試験（その理由を含む）をまとめた報告書（「試験完了報告書」）を作成しなければなりません。不具合や実装が延期された機能については、未解決の問題に対する是正策とともに文書化しなければなりません。

シティからの要請があった場合、サプライヤーは以下の証拠を提出しなければなりません。

1. 詳細なテスト計画
2. テスト終了レポートに詳細が記載されているテスト完了および結果
3. テスト結果と要件およびコードのコミットとのトレーサビリティ

17.33 デプロイメント

デプロイメントに先立ち、サプライヤーは、脆弱性スキャンや脅威モデリングを含む、必要なすべてのセキュリティテストを完了しなければなりません。リリースプロセスには、変更記録、ロールバック戦略、および必要な承認手続きを文書化した体制を

整備しなければなりません。実施計画および導入ランブックには、監視およびエスカレーション手順を盛り込む必要があります。

導入後、サプライヤーはシステム識別子を確定し、監査対応が可能な状態を確保するため、関連するすべての成果物を更新しなければなりません。

17.34 セキュリティ

1. SDLC の設計段階で、コードが記述される前に潜在的なセキュリティリスク、脆弱性、およびアーキテクチャ上の弱点を特定し、対処するための体系的な評価（「セキュリティ設計レビュー」）を SDLC に組み込むとともに、OWASP などの業界標準に準拠した予防的および検知的な統制措置を講じなければなりません。
2. セキュリティ保護されたコーディング慣行の実践が必要です。
3. サプライヤーは、アプリケーション、商品、サービスの選択、開発、実装のプロセスと手順に情報セキュリティコントロールを取り入れる必要があります。
4. サプライヤーは、シティの情報が保存、処理、および/または送信されるすべてのシステムについて、安全な構築手順を整備し、すべてのシステムに対して安全なイメージまたはテンプレートを維持しなければなりません。

17.35 マルウェア対策

サプライヤーは、悪意あるコード（ウイルス、ワーム、トロイの木馬ウイルス、アドウェア、スパイウェア、ランサムウェアまたはデータが漏洩する可能性のある、同様の性質のその他のサイバー攻撃）の侵入を防止し、検出するための適切な措置を講じて、その実施を確実にする必要があります。サプライヤーは以下を行う必要があります。

1. すべてのパソコン、ローカルエリアネットワーク（LAN）サーバー、メールサーバー、シティのデータを保管、処理および / または送信するその他のデバイスでウイルス防止およびスパイウェア防止テクノロジーを実施、更新、維持します。
2. セキュリティ設定を装備し、エンドユーザーによるウイルス防止/マルウェア対策ツールおよび定期的なスキャン機能の無効化を防止します。

3. ウイルス防止およびマルウェア対策ソフトウェアの設定と更新の集中管理自動化手順を設置します。
4. ウイルス防止シグネチャーまたはスキャンエンジンが古い不適合コンピュータを特定し、これに対応するためのプロセスが必ず実装されているようにします。
5. ストレージメディアを含むがこれに限定されない外部デバイスへの接続を可能にする通信ポート/インターフェイスへのアクセスを制御します。

17.36 モバイルコード対策

サプライヤーは、安全なモバイルコードの実践に関するコントロールの導入を確保する必要があります。モバイルコードの使用が許可されている場合、その設定は最低でも関連するすべての業界基準とシティへの契約義務を満たしている必要があります、サプライヤーは、許可を受けているモバイルコードが明確に定義され文書化されたセキュリティポリシーに従って運用され、不正なモバイルコードの実行を防ぐことを徹底してください。

基盤となるオペレーティングシステムまたはプラットフォーム（「サンドボックス」外など）に影響を与える可能性のあるモバイルコードについて、サプライヤーは以下を保証する必要があります。

1. サプライヤーの発行するモバイルコードは、シティの承認した認定機関が署名し、サプライヤーは証明書のライフサイクルを管理して、証明書の期限切れやローテーションに対応するものとします。
2. 証明書の期限が切れた署名入りモバイルコードは実稼働環境から削除する必要があります。

17.37 監査ログ

サプライヤーは、シティのデータのアクセス、保存、処理、管理、および/または送信に使われる規制情報システムがすべて、インフラストラクチャまたはアプリケーションレベルで監査トレイルを維持し、以下の項目をログしていることを確認する必要があります。

1. 関連のあるプラットフォームのインフラセキュリティ関連のアクション
2. ファイアウォールまたは IDS / IPS によって生成されたセキュリティイベントに関連するすべてのシステムアラーム

3. すべてのシステムセキュリティに違反する試み（ユーザーログイン試行の失敗など）
4. リソース（ソフトウェア、データ、プロセスなど）への不正なアクセスの試み
5. 管理者のアクション
6. ユーザーまたは他のシステムからの特定情報の受領に関する情報
7. 金融取引とシティの情報に関わるすべての重大な事象（特に以下の項目が含まれているもの）
 - a. 金融取引に対する更新
 - b. 機密 PII または極秘 PII データに対する更新
 - c. 極秘データに対する更新
 - d. 認証データに対する更新
8. 確立されたすべてのセッション
9. 技術的に可能で、シティのアプリケーション（ウェブサイトおよびモバイルアプリケーション）で記録されているときは、一意のデバイス ID などのセッションアーチファクトをキャプチャして、詐欺調査を支援する必要があります。これらの成果物には少なくとも IP アドレスが含まれていなければいけません。このようなアーチファクトは、シティの取引とシティの口座開設活動で取得するものとします。情報は、セッションアーチファクトを取引または口座開設に関連付けられるよう取得する必要があります。
10. 監査証跡は、報復を防止するために、特定のアクティビティが特定の個人に帰属することを文書化する必要があります。
11. 重大な情報セキュリティ管理（ISA）イベント、特に以下の項目を含むものはログしなければなりません。
 - a) ユーザーの作成
 - b) ユーザーアクセス権の変更
 - c) 規制情報システムでのプロフィールの削除、作成、変更
 - d) パスワードのリセット
 - e) システムセキュリティ設定の変更
 - f) 権限のある職務 ID のインタラクティブなすべての活動

- g) 含めることが技術的に不可能でない限り、ログを生成しているシステムに関わらず、セキュリティログには、最低でも以下の情報を含める必要があります。
- I. イベントの日時（UTC フォーマットの時刻）
 - II. アクションを実施している個人のユーザーID
 - III. イベントの種類
 - IV. 影響を受ける資産またはリソース名
 - V. アクセスの種類（削除、変更など）
 - VI. イベントの成否
 - VII. ソース（端末、ポート、場所、IP、ホスト名など）

17.38 ログ情報の保護

サプライヤーは、開始時、シャットダウン時、保管時、送信時に、監査証跡の完全性を維持するため、アクセス制御の実施を確保する必要があります。

1. 監査ログへの不正な変更を防ぐため、サプライヤーは、アクティビティを追跡しているシステムユーザーがログを上書きまたは変更できないようにする必要があります。
2. サプライヤーは、データの維持方法を定義し、適用されるすべての法的および規制要件を参照するコンプライアンス対策を含むログデータの記録保持手順をシティに提供する必要があります。
3. 組織内またはセキュリティドメイン内のすべての情報処理システムの時計は、正確な情報源の時刻と同期していなければなりません。

17.39 監視システムの使用

サプライヤーは、以下のイベントが、必ず、直接または自動レビュープロセスによってキャプチャ、ログ、レビューされるようにする必要があります。

1. ファイアウォールまたは侵入検知システム（IDS）/侵入防止システム（IPS）によって生成されたセキュリティイベントに関連するすべてのシステムアラーム。
2. 安全な基準構築で特定された重要なリソースのすべての更新。

3. 機密 PII またはそれ以上に分類される情報にアクセスして、あらゆる ID（機能 ID、特権 ID、システム ID、一時 ID など）が実行するすべてのインタラクティブな活動。
4. 以下の例外を除く、上記の「監査ログ」セクションに記載されている重大 ISA イベント。
 - a) エンドツーエンド統合管理機能のある自動ワークフロー / フルフィルメントシステムで情報セキュリティ管理活動が実行される場合、ユーザー、役割、またはプロフィールからの資格の削除。

17.40 ログの相関関係とレビュー

1. ログに記録されたイベントによりアラートが発生した場合は、サプライヤーは、イベントを審査し、有害な情報セキュリティインシデントが発生した可能性が示された場合は追跡活動と調査を実施しなければなりません。
2. サプライヤーは、監査ログがセキュリティ情報およびイベント管理（SIEM）システムなどの中央ログ管理システムに集計されるようにするか、ログの相関関係分析とレビューのためログ分析ツールに集計されるようにしなければなりません。
3. サプライヤーは、定期的に審査を行い、その SIEM またはログ分析ツールの設定を調整して、対策が可能なイベントの特定を向上するものとします。

17.41 業務ソフトウェアの管理

サプライヤーは現在、業界の認定している業務用プロバイダーがサポートしているか、セキュリティの問題に対応可能なアクティブで適切なパッチと設定更新のリリースがあるオペレーティングシステムとソフトウェアのみを活用する必要があります。

サプライヤーは、承認されたセキュリティパッチおよび設定のすべてを適用する是正措置の実施期間を指定する文書化されたプロセスが必ず実施されているようにするものとします。

サプライヤーとシティ間で別個のメンテナンス契約があるかどうかにかかわらず、サプライヤーは、シティのために開発され、ライセンス契約で管理されるソフトウェアが、既知の脆弱性を有する非サポートソフトウェアのバージョンを使用する許可がな

く、かかるソフトウェアは必要に応じて適時に更新およびパッチ適用を行うことを保証しなければなりません。

シティの情報の処理に使用されるアプリケーションソフトウェアは、確立されたサプライヤーから入手し、ライセンス供与され、カタログ化、サポートされなければなりません。

17.42 脆弱性および脅威管理

1. サプライヤーは、以下すべてに包括的に対処した、および/または含んだ脆弱性・脅威管理プロセスを実施しなければなりません。
 - a. シティの機密またはより機密性の高いデータの処理、保存、アクセス、または送信に使用される可能性のあるすべての資産における脆弱性の発見および管理のためのツールおよび手順。
 - b. 業界で認められた脆弱性検査ツールおよび報告手法を用いて、少なくとも週1回はスキャンを実施すること。
 - c. 最新バージョンの「共通脆弱性評価システム (CVSS)」 (<https://www.first.org/cvss>を参照) に従う強度に基づいた脆弱性の順位付けと修正スケジュール。
 - d. 完全なプロダクション展開前の脆弱性修正テストの義務付け。
 - e. 重要な脆弱性の修正を加速するための、文書化された反復可能な運用プロセス。
 - f. サプライヤーは、資産のサポート対象となるライフサイクル全体を通じてその状況を追跡し、製品寿命終了 (EOL) またはベンダーサポート終了 (EOVS) の状態に備えるとともに、当該資産を先を見越してアップグレードまたは交換するためのプロセスを整備しなければなりません。
 - g. 情報収集、脆弱性スキャン、または侵入テストを通じて特定された重要な CVSS スコアリング脆弱性は、優先順位を付け、脆弱性リスクに見合った明確な期限内に是正されなければなりません。

17.43 第三者がホスティングするアプリケーション

サプライヤーがシティの機密データ、または機密性の高いデータを、ウェブサイトまたはインターネットアクセス可能なシステム、またはシティのブランド名が付いているウェブサイトで維持または保管する場合、シティに影響を与える商品またはサービスに関わる脆弱性または脅威（それぞれ「脆弱性」）から保護するために、サプライヤーは以下の要件を遵守する必要があります。

1. サプライヤーの従業員1名を任命し、情報セキュリティに関するシティからの問い合わせに対応させること。
2. FIRST、CERT/CC、CISA 既知の悪用された脆弱性のカタログ、ベンダーのメーリングリストなどのコンピュータセキュリティの脆弱性に関する定評ある情報源を週1回以上の頻度で監視し、関連するサービスパック、パッチ、アップグレードおよび回避策を入手、徹底的にテスト、適用し、シティに提供するために適切な措置を取る、業界が最善と認識することを活用すること。
3. 四半期に1回以上の頻度で、ネットワーク、システム、アプリケーションの脆弱性スキャンツールおよび/または侵入テストを用いて、情報セキュリティ対策の実施状況をテストすること。
4. サプライヤーが何らかの契約上の義務および本要件を遵守していることを確認するため、シティまたはシティが承認したサードパーティに、適切な間隔で、脆弱性評価、倫理的ハッキングまたはその他のセキュリティ評価を行うことを許可します。これは、ポリシー、プロセスおよび手順のレビュー、物理的セキュリティ配置、ネットワーク、システムおよびアプリケーション脆弱性スキャンおよび侵入テストのオンサイト評価、およびこうした検査を実施するための市販のツールおよび/または業界基準の慣行を使用した侵入テストを含むが、これに限定されないものとします。
5. サプライヤーに脆弱性評価サービスを提供する業務委託先は、シティが承認した脆弱性評価プロバイダーのリストに記載された業務委託先でなければなりません。サプライヤーが本サービスを提供するために業務委託先または業務委託先を利用する場合、サプライヤーは、自己の費用で、要求される脆弱性評価が、サプライヤーが直接サービスを提供する場合と同様にタイムリーに完了するようにし、業務委託先または業務委託先がかかる評

価を促進する要件は、シティがかかる評価を行う権限を与える文言を含め、サプライヤーと業務委託先/業務委託先の間のサービスに係る契約において明確にされなければなりません。

6. 通知

- a) サプライヤーが、シティに影響を与える商品またはサービスに関わる脆弱性を特定した場合、サプライヤーは、特定後 24 時間以内にシティに書面で通知し、サプライヤーが行っている是正措置の説明を含めなければなりません。
- b) サプライヤーが、シティに影響を与える商品またはサービスに関わる脆弱性を、プロセスチャネルの責任ある公開（国家脆弱性データベース（NVD）への公表、または外部セキュリティベンダーに提供する脅威カタログ経由）により知った場合、サプライヤーはその公表から 24 時間以内にシティに書面にて通知するものとします。各通知には、脆弱性についての情報、シティ関連サービスに対するシステムの有用性（すなわち、シティの情報をホストしているか、サービスの提供に使用されているか、またはその両方）、リモートで悪用できるかどうか、共通脆弱性識別子（CVE）スコアが含まれます。サプライヤーは、本脆弱性が是正されるまで、シティに対して更新情報を提供し続けるものとします。シティが脆弱性を特定した場合、シティはサプライヤーにその旨を通知することができ、サプライヤーは本セクションに従い、速やかに脆弱性を是正するものとします。

7. **改善策** 本セクションに基づき提供された各脆弱性について、通知当事者は当該脆弱性の重大性とシティに対するリスクに基づき、リスクレベルと影響を評価し、その付録 A に定める共通脆弱性評価システム(CVSS)に基づきリスク優先度を割り当てます（<https://www.first.org/cvss> を参照）。両当事者によりリスクレベルが割り当てられ、合意されると、サプライヤーは、特定された中、高、または重要な脆弱性を修正するものとします。可能であれば、そのような脆弱性の修正は、現在配備されているリリースに対してセキュリティパッケージとして利用できるようにする必要があります。

サプライヤーが、シティが満足するように脆弱性を修復できない場合、または修復する意志がない場合、シティは、（修復された部分について）それ以上の責任または金銭的義務なしに該当するライセンスを解除でき、サプライヤーは、支払われたライセンス料の日割り分をシティに速やかに払い戻すものとしします。

17.44 コミュニケーションセキュリティ ネットワーク コントロール

1. シティ情報のアクセス、保管、管理、処理、および/または送信に使われるサプライヤーのネットワークを脅威から保護し、ネットワーク内の実施ポイントを使用する情報システムのセキュリティを維持する必要があります。
 - a. シティの情報分類が機密またはそれ以上である情報は、インターネットに面した非武装地帯（DMZ）内のシステムに永続的に保存してはなりません。不正アクセスを防ぐための適切な対策を含むワイヤレスローカルエリアネットワーク(WLAN)または他のワイヤレスデバイスソリューション(PEAP-TLS、EAP-TTLS など)を使用してシティの情報にアクセス、保存、管理、処理、および/または送信するために使用されるネットワークは、シティの情報が含まれるネットワークに接続できます。
 - b. サプライヤーのグローバルネットワークへの外部 IP 接続がすべて、サプライヤーの管理するファイアウォールで保護されていること。
 - c. シティ情報がアクセス、管理、保存、処理、または送信されるサプライヤーのネットワークへのインターネット接続を監視および保護する、侵入検出システム(IDS)および侵入防止システム(IPS)がリアルタイムで実行されていること。
2. シティのブランドを使用したインターネットアプリケーションすべてについて、サプライヤーは以下を保証しなければなりません。

- a. サプライヤーのサイトでホスティングされているサービスは、シティの承認した DDoS（分散型サービス拒否）予防サービス、またはシティの承認した類似対策で保護されます。
- b. 外部ファイアウォールは、「デフォルトで拒否」のルールで設定しなければなりません。ファイアウォールルールは最低権限原則に基づいて設定されなければならず、ファイアウォールに拒否されたすべての接続試行（パケットドロップなど）は、ログに記録されなければなりません。
- c. ネットワーク通信はデフォルトで拒否され、管理インターフェイスでは例外的に許可されなければなりません。例外は、特定のソース、目的地、およびサービスに非常に限定されなければなりません。
- d. ウェブアプリケーションのトラフィックには、ウェブアプリケーションファイアウォールなどを通じて、適切な制御とフィルタリングを行う必要があります。

17.45 ネットワーク内での分離

サプライヤーは、シティの情報へのアクセス、保存、処理、管理、および/または送信に使われる規制情報システムがすべて、インフラストラクチャまたはアプリケーションレベルで監査証跡を維持し、以下の項目をログしていることを確認する必要があります。

緊急時には、サプライヤーはネットワークのセキュリティイベント（ウイルス発生時のポートのフィルタリングなど）の影響を抑えられるよう、ネットワークの部分間のアクセスをフィルタリングできる必要があります。

リモートアクセスとホストセキュリティはグループベースのアクセス制御（スタッフ、業務委託先など）を実施し、サプライヤーネットワークのネットワークリソースへのアクセスを制限する必要があります。ホストレベルでは、グループレベルまたは個人レベルでアクセス制御を実施できます。

17.46 ネットワーク内の機器の識別

テクノロジープラットフォームは、インタラクションの IS リスクレベルやその他の緩和コントロールに見合った、ピアテクノロジープラットフォームを識別し、認証するものとします。

1. サプライヤーのデバイス（デスクトップ、ノートパソコンなどのハードウ

ウェアが含まれますが、これらに限られません）のみが、シティの情報が保管、処理、または送信されるサプライヤーのネットワークにアクセスできます。

2. これらの要件を遵守し、シティが許可しているサプライヤーのデバイス（デスクトップ、ノートパソコン、リムーバブルデータストレージメディアなどのハードウェアが含まれますが、これらに限られません）のみが、シティのネットワークにアクセスできます。

17.47 セキュリティ要件の分析と仕様

サプライヤーは、アプリケーション、商品、サービスの選択、開発、実装のプロセスと手順に情報セキュリティ手順を取り入れる必要があります。

17.48 オンライン取引

1. 適宜、サプライヤーはログイン資格の確認のために、動的なパスワードまたはデジタル証明書を使用する情報システムが必要です。
2. すべてのエンドエンティティ証明書は、少なくとも 13 か月に一度交換する必要があります。
3. シティ情報の保管、処理、管理、またはアクセスを行う、インターネットに接続するシティブランドアプリケーションをホスティングする、またはシティのネットワークリソースに接続するサプライヤーアプリケーションには以下が必須となります。
 - a. アクセスされるデータ/機能のタイプに基づいて認証方法を活用。
 - b. マルチファクター認証(MFA)コンプライアンス評価の実施と、必要に応じた推奨事項の実装。
 - c. 疑わしいアクティビティモニタリング(SAM)オンボーディング評価の実施と、必要に応じた推奨事項の実装。
 - d. これらすべての場合、サプライヤーは、シティの現在の要件について、主要な連絡窓口に問い合わせるようにしてください。

17.49 変更管理手順

1. サプライヤーは、ファイアウォール、侵入検知システム（IDS）、侵入防止システム（IPS）に対する設定変更が、サプライヤーの変更管理プロセスに送られるように徹底するものとします。

2. 一時的な ID を使用して行われた実稼働環境へのアクセスは、環境への変更を追跡できるようログしてモニタリングする必要があります。
3. シティの情報分類が「機密」以上、または IS リスクコンポーネント値が「整合性」、または「可用性」が「高」の顧客情報が含まれている規制情報システムでは、サプライヤーはセクション 17.32（監査ログ）に従ってキャプチャされたログをレビューしなければなりません。このようなレビューは、適切なリスクベースのサンプル抽出方法に基づいて行うことができます。
4. レビューでは、一時的な特権アクセスの一環として行われる変更が意図されたとおりに行われたことを確認する必要があります。
5. サプライヤーは、レビュープロセスの証拠の保管を含め、すべての変更を文書化する必要があります。

17.50 情報漏洩

サプライヤーは、情報漏洩を防ぐため、以下を含む安全なコーディング基準を策定しておく必要があります。

1. 詳細なシステム情報（サーバーのタイプ、テクノロジーなど）
2. ディレクトリのツリー構造と基礎となるデータベースのタイプを示すスタックトレースおよび例外エラー

17.51 テストデータ

シティの情報分類が機密またはそれ以上である情報は、業界基準を満たすツールおよび方法を使用して匿名化、マスク化、および/または難読化され、そのデータが機密ではなくなる場合を除き、サプライヤーがソフトウェアアプリケーションの開発環境またはテスト環境またはラボでサプライヤーによって使用または保存されないものとします。または、サプライヤーが開発環境またはテスト環境内で実稼働管理を実装する必要があります。

17.52 システムの受諾

サプライヤーは、適切な業界基準を満たすプロジェクト範囲管理およびシステム受諾プロセスを策定して文書化する必要があります。

17.53 情報セキュリティ脆弱性の報告

サプライヤーは、シティの情報資産に危険が生じるようなアプリケーションならびにインフラの脆弱性について速やかにシティに報告できるプロセスを策定しておかなければなりません。

17.54 セキュリティインシデントの責任と手順

1. SIRT は、セキュリティインシデントがどのように起こったか、またはどこで起こったか、または侵害を引き起こした可能性があるかにかかわらず、以下のいずれかを侵害するセキュリティイベントを指します。
 - シティのデータの機密性、完全性、または可用性
 - シティが契約上、法律上、または規制上の義務を負うあらゆるデータ（個人情報を含む）の機密性、完全性、または可用性
 - シティのデータを保存、処理、または送信するシティの情報システムの完全性または可用性
2. 本稿において、「機密性の侵害」とは、権限のない者にデータが漏洩すること、またはシティが当該データの保管および管理権限を失う事態を指します。すべてのセキュリティインシデントは、直ちに報告されなければなりません。
3. サプライヤーが SIRT を経験した場合、サプライヤーは、シティ独自のインシデント対応プロセスに基づきシティから要求された情報の提供に協力し、シティが法的、規制上、および/または内部ガバナンス上の要件を満たせるよう、侵害されたデータを十分に分析しなければなりません。法律、規則、または規制に基づき要求される、あるいはシティが裁量に基づき希望するあらゆる通知を、シティの要請に基づき、サプライヤーの費用負担で実施すること。ただし、シティが提案された通知テンプレートの文言を審査し、修正する機会を得た後に限ります。また、サプライヤーは、シティが書面により明示的にその記載を要請した場合を除き、かかる通知においてシティの名称を記載してはなりません。

17.55 データ漏洩防止(DLP)

サプライヤーは、シティ情報分類が「機密」以上のデータにアクセスする全スタッフを対象とするコンテンツとエンドポイントモニタリングを含む、データ漏洩防止(DLP)制御を実施する必要があります。

サプライヤーは、以下の経路を通じたシティの機密またはそれ以上のデータのネットワークからの移動を検出および防止する制御を設置するものとします。

- a. 暗号化されていない E メール
- b. 暗号化されている Eメールの添付ファイル
- c. シティデータの印刷
- d. ネットワーク外の場所へのシティデータの転送（FTP を通じてなど）
- e. USB ドライブ、リムーバブルハードドライブ、CD/DVD ドライブ、およびその他データ保存機能を持つリムーバブルデバイスなどのリムーバブルメディアに、シティの情報分類が「機密」以上のデータをコピーしようとする。この特権をデフォルトで禁止する必要があります
- f. DLP ソリューションは、シティの機密またはそれ以上のデータをネットワークからその他の場所へ移動、転送、またはコピーする試みに相当するすべてのイベントのログを作成し（その成否を問わず）、サプライヤーにアラートを送信するものとします。この特権をデフォルトで禁止する必要があります
- g. SaaS/ファイル共有サイトを含む外部ウェブサイトへのシティデータのアップロード。この特権をデフォルトで禁止する必要があります

17.56 ウェブブラウジング

1. サプライヤーには、シティのデータにアクセスする従業員によるシティ情報分類が「機密」以上のデータの共有、およびマルウェアや攻撃にさらされることを防ぐための制御対策がなければなりません。
2. シティの機密またはそれ以上のデータにアクセスするサプライヤーには、以下のことが求められます。
 - a. すべての URL リクエストはログに記録されなければなりません。
 - b. シティのデータを不正に共有するために使用される可能性のあるサイト（ウェブメール、チャット、ソーシャルメディア、オンラインストレージ、Gen-AI など）へのアクセスはブロックする必要があります。
 - c. マルウェアや攻撃にさらされる可能性のある環境にあるサイトへのアクセスはブロックしなければなりません。
 - d. 業務に関係がないとみなされるサイトへのアクセスはブロックしなければなりません。
 - e. サプライヤーは、定期的に更新される URL 分類サービスに登録しなければなりません。分類されていないすべての URL をデフォルトによりブロックするか、すべての URL をデフォルトによりブロックしてケースバイケースで承認する必要があります。
 - f. サプライヤーが使用しているウェブブラウザは完全にサポートされているもので、ソフトウェアベンダーが提供する最新のセキュリティアップデートで更新する必要があります。

17.57 電子メッセージ

インスタントメッセージ、ピアツーピアネットワークなどのインターネットコラボツールは、第 17.9 項（暗号化制御の使用に関するポリシー）に従ってすべてのシティのデータについて適切な暗号化が行われているのでない限り、サプライヤーのネットワーク外で、あるいは、シティの情報が含まれているネットワークからシティの情報の送信や保存に使用できません。

17.58 E メール

サプライヤーには、シティの情報の共有、およびマルウェアや攻撃にさらされることを防ぐための E メール制御がなければなりません。これには次の事柄が含まれます。

1. Eメールゲートウェイに入ってくる受信添付ファイルをスキャンし、システムにリスクをもたらす場合はブロックします。
2. Eメールフィルタリング（スパム防止、フィッシング対策）ソフトウェアを使用し、常に最新のものにします。
3. シティの機密またはそれ以上のデータを組織外に送信する際は、すべて暗号化するものとします。
4. サプライヤーが使用しているEメールクライアントは完全にサポートされているもので、ソフトウェアベンダーが提供する最新のセキュリティアップデートで最新のものにします。

17.59 リムーバブルメディア

1. サプライヤーは、シティの情報が保持されているメディアのタイプに関わらず、シティの情報を保護するものとします。この基準は、情報が保存される以下のメディアに適用されますが、これに限定されません。カード、カセット、コンパクトディスク（CD）、チェックストック、ディスケットなどのリムーバブルストレージデバイス、ハードコピー出力、磁気ディスク、磁気テープ、マイクロフィルム、マイクロフィッシュ、光ディスク、紙媒体の文書。
2. シティの情報が保存されているシステムのポータブルメディア/ストレージデバイスへのアクセスのデフォルト設定は、アクセス不可となっていなければなりません。例外で読み取り・書き込みアクセスが許可される場合は、ポータブルメディアデバイスでデータを暗号化する必要があります。
3. リムーバブルメディアの使用が許可されている場合、その使用にはリムーバブルメディアの使用を必要とするビジネス上の根拠を含む、経営陣からの承認プロセスが必要です。リムーバブルメディアについては管理者がインベントリを作成しなければなりません。シティの機密またはそれ以上のデータが含まれるリムーバブルメディアは、ユーザーによる操作を必要とせずに自動的に暗号化されなければなりません。

17.60 メディアの処分

1. シティの情報分類が「機密」以上のシティの情報を、シティの指示に従い処分する場合（当該情報が不要になるかシティにとって利用価値がなくなった時点、またはシティにとって有用でなくなった時点に加え、法律、規

制および/またはシティのポリシーにより要求される追加的な保存期間が満了した時点)、サプライヤーは、当該情報を使用不能かつ回復不能な方法で破棄する必要があります。

2. 以下のルールに従って、取り付け可能なメディアを安全に消去するには、ドライブのセクタをランダムに特定の異なる文字で上書きする承認されたツールを使用する必要があります。
 - a. シティの情報分類が「機密」以上の情報が保存されているメディアについては、メディアにツールを 3 回使用するものとします。
 - b. 該当する場合、メディアをデガウス（磁気消去）します。
3. メディアを物理的に破壊して、読み取り不能にします（ドライブをシュレッダーにかける、粉碎するなど）。
4. シティの情報分類が「機密」以上の情報が含まれた紙やその他の非電子ストレージメディアは、安全に回収し、最終的な廃棄まで安全な機密文書用廃棄容器に保管する必要があります。機密文書用廃棄容器は常に鍵をかける必要があります、権限のある従業員のみが可能である必要があります。
 - a. シティの情報分類が「機密」以上の情報が含まれている可能性のあるメモリ/ストレージ機能付きのコピー機、プリンター、ファックス、その他の機器もサニタイズする必要があります。

17.61 情報セキュリティ管理とトレーニング

1. フィッシングなどのソーシャルエンジニアリング攻撃の防止、分類が機密情報およびそれ以上の情報の適切な取り扱い、セキュリティインシデントの報告・対応管理等を含む（ただしこれらに限定されない）サイバー/情報セキュリティに関する適切な啓発・教育プログラムを維持するものとします。
2. サプライヤーは、業務委託先や臨時スタッフを含むすべての従業員が、各自の職務に関連する組織のポリシーおよび手順に関する適切な意識向上教育とトレーニングを受けていることを確認するものとします。
3. サプライヤーは、サイバーセキュリティ分野における新たなリスクや脅威、最新のベストプラクティス、および新技術に対応するため、研修および啓発プログラムが毎年見直され、更新されるよう確保しなければなりません。
4. 少なくとも、以下のトピックを含める必要があります。
 - b. 情報のラベル付けと取扱い
 - c. 安全な送信（安全な E メール、安全な SharePoint ストレージ、シティ所有データを個人の E メールに送信しない）
 - d. 情報セキュリティインシデント報告
 - e. 安全な職場（適切なインターネットの使用、認可されていないソフトウェア、承認されていないソフトウェアのダウンロードを禁止など）
 - f. パスワード管理（強力なパスワード、パスワード共有の禁止など）
 - g. ソーシャルエンジニアリング（フィッシング、スパイフィッシング、ビッシング、スミッシングなど）
 - h. リモート通勤（セキュア/安全な接続、個人デバイスのセキュリティなど）

5. サプライヤーの従業員は、シティのデータをホスティングするシステムにアクセスする際、またはアクセスする前に、トレーニングを受け、配属通知に記載された期日までにトレーニングを完了しなければなりません。
 - a. IS トレーニングは、法律で禁止されていない限り、少なくとも年 1 回すべての従業員に実施する必要があります。
6. 現地の法律で認められている限り、トレーニングにはその効果を測定・記録するための成果物（修了時の可否の基準値を設けた小テストなど）を含める必要があります。

17.62 サイバーリスク管理プログラム

また、サプライヤーは、最低限、以下を含む適切なサイバーリスク管理プログラムを維持しなければなりません。

1. 明確に定義され、文書化された、情報セキュリティリスク管理プログラム、および/または、サイバー/情報リスク管理の要素が明確に定義されたオペレーショナルリスク管理プログラムを維持し、サプライヤーのサイバーリスク選好度を定義し、サイバー残留リスクとその選好度の整合性を確保すること。
2. 強固なセキュリティリスク管理のガバナンスプログラムを維持すること。
これには、組織内のセキュリティの全体的な状態を評価するセキュリティ監査とレビューの収集および/または実施、並びにサプライヤーのサイバーリスク選好度に違反していないことの確認と保証のために少なくとも年 1 回経営幹部に報告することが含まれるが、これに限定されないものとします。
3. サプライヤーがクレジットカード/デビットカード取引、支払い、および/または情報を処理、保存、および/または送信する場合、サプライヤーに適用されるあらゆる PCI データセキュリティ基準（PCI-DSS）の遵守を維持すること。
4. サプライヤーが、危機管理計画とプレイブックと業界基準に沿ったセキュリティインシデント対応チーム計画を維持し、サイバーセキュリティインシデントの試み、疑い、実際の事故を検知、抑制、調査、対応、回復するための十分かつ適切な能力をサプライヤーが有することを保証すること。

17.63 アプリケーション、API、コード、システム、インフラストラクチャのセキュリティ

サプライヤーがソフトウェアアプリケーションのホスティング、開発、共同開発、開発環境の提供、および/または供給を行っている場合、サプライヤーは、セキュリティ上の欠陥、不正アクセス、改ざん、および/またはマルウェアまたはその他の形態の悪意のあるコードの挿入の防止を目的とする当該ソフトウェアのコードレビューおよび/またはソフトウェアのパッチ、並びにアプリケーション（APIを含む）とその基盤となるシステムサービス、オペレーティングシステム、ネットワークに、セキュリティインシデント、プライバシー侵害、不正行為、不正アクセスおよび/または機密情報の開示、本アプリケーションにより処理、保存または送信されている情報の整合性の喪失、および/またはサプライヤーがシティに提供する製品またはサービスの品質に影響を与える可能性のある可用性の喪失につながり得る既知の脆弱性および欠陥のないことを確認するための脆弱性テストを実施するものとします。

17.64 モバイルセキュリティ

サプライヤーがモバイルアプリソリューションを提供する場合、サプライヤーは以下の要件を遵守するものとします。

1. モバイルアプリケーションは、Google Android（Android Goを除く）および/または Apple iOS / iPad OS プラットフォームの一般に入手可能な（GA）/安定しており、かつ EOL でない²バージョンのみをサポートする必要があります。モバイルソリューションが追加のサポート機能を備えている場合、サポートされているオペレーティングシステム/バージョンをシティが設定できるものとします。
2. モバイルソリューションは、本文書のセクション 17.9（暗号化要件）で規定された暗号化を含むがこれに限定されない暗号化アルゴリズムをサポートする正規の指示セットが装備されていないモバイルプラットフォーム/デバイスをサポートしてはなりません。

²積極的にサポートされ、プラットフォーム所有者またはサプライヤーから定期的なセキュリティとメンテナンスの更新を受けている製品バージョン。

3. ベータ版、早期アクセス版、機能プレビュー版/リリースを含むがこれに限定されない量産前のオペレーティングシステムのバージョンは、実稼働環境では使用できません。
4. サプライヤーは、モバイルソリューションによってバンドル/活用される無料かつオープンソースのソフトウェアライブラリを含むがこれに限定されない、統合されたサードパーティのコンポーネントのリストを提供できなければなりません。
5. モバイルアプリケーションは、Apple の App Store や Google Play ストアなどの公開アプリストアを通じてモバイルアプリケーションを公開できるようにする要件とベストプラクティスを遵守するものとします。記載された公開アプリケーションストアは、モバイルアプリケーションの配布/公開を優先し、主な方法とするものとします。
6. Android モバイルアプリケーションでは、APK 署名スキーム v2+を活用する必要があります。APK 署名スキームバージョン 1（別名：JAR 署名）を使用してはなりません。
7. モバイルアプリケーションの署名キーの種類と長さは、本文書のセクション 17.9 - 暗号化要件を遵守しなければなりません。
8. 各アプリケーションの署名キーと関連する X.509v3 証明書は、個別に管理し、単一のアプリケーション ID/バンドル ID 専用でなければなりません。署名キーをアプリケーション間で共有してはなりません。
9. モバイルアプリケーションがモバイルデバイス上のデータの保持を必要とする場合、アプリ/サービスの目的に必要なデバイス上の最新のデータ、または法的または規制要件に従って必要な場合にのみ保持する必要があります。
 - a. ユーザーデータの収集、処理、および/または保管は、一般データ保護規則（GDPR）および 2002/58/EC（ePrivacy）指令、またはそれ

らに相当する地域などのプライバシー規制を含む（ただし必ずしもこれらに限定されない）現地の法律を遵守する必要があります。

- b. 統合されたサードパーティのコンポーネント（ライブラリなど）は、ユーザーデータを収集、処理、および/または保存してはなりません。

10. モバイルアプリケーションでは、いかなるアプリケーションデータも、世界からアクセス可能にすることはできません。

- a. 他のアプリケーションとデータを共有する必要がある場合、アプリケーションは各オペレーティングシステムで商業的に妥当な技術、方法、およびコントロールを活用し、そのようなデータ共有が適切に正当化かつ文書化される最小数の他のアプリケーションと必要な量のデータのみを共有する必要があります。

11. モバイルアプリケーションは各モバイルオペレーティングシステムが提供するセキュアな通信機能のみに依存しなければなりません。例えば、以下の通りです。

- a. **Android** アプリケーションでは、アプリケーションマニフェストおよび/またはネットワーク設定ファイルのネットワークドメインに対して、セキュアではないネットワークトラフィックが許可されていないことを明示的に宣言する必要があります。
- b. **iOS/iPad OS** アプリケーションでは、例外なく、アプリケーショントランスポートセキュリティ（ATS）を活用する必要があります。

12. 暗号化資料は、ハードウェアでバックアップされた安全なキーストアに結びついている必要があります。

13. モバイルアプリケーションはリリースモードでビルドする必要があり、以下を含めてはなりません。

- a. セキュリティコントロールを回避できる機能または方法
- b. ソースコードのファイル名、変数名、シンボル名、コメントなど、リバースエンジニアリングを容易にする可能性のあるデバッグ情報

14. モバイルアプリケーションには、実行時にアプリケーションの動作を変更または監視できる可能性のある、悪意あるコードの注入を防ぐための効果

的なフッキング防止または改ざん防止メカニズムが装備されている必要があります。

15. モバイルアプリケーションでは、リバースエンジニアリング攻撃を阻止するために、包括的なデバッグ防止またはリバースエンジニアリング防止/難読化技術を実装する必要があります。
16. モバイルアプリケーションパッケージには、そのコンテンツの信頼性と完全性を検証できる機能（暗号化チェックサムやデジタル署名の使用など）が装備されている必要があります。
17. モバイルアプリケーションがユーザー認証を必要とする場合、ユーザー認証を開始する前にアプリケーションおよび/またはデバイスの整合性チェックを完了する必要があります。
18. シティの分類が「機密」以上のシティが所有する情報および/または IS リスク分類が「中」以上のシティが所有する情報にアクセス/処理/保管するモバイルアプリケーションは、強固な生体認証モダリティ（例えば、対応する [Android 互換定義文書](#) で定義されているクラス 3/強固なカテゴリを満たすまたは上回る）のみを活用する必要があります。
19. モバイルアプリケーションは、中間者（MitM）攻撃から保護するための対策を実施する必要があります。
20. モバイルアプリケーションは、「ジェイルブレイク」または「ルート化」されたモバイルデバイスを含むがこれに限定されない、侵害されたデバイスを検出し、ビジネスのリスク評価および規制要件に従って対応する必要があります。
21. モバイルアプリケーションは、ソフトウェアトークン（所有の証明など）のクローン化を防ぐための強力なデバイスバインディングを実装する必要があります。
22. モバイルアプリケーションは、セキュアなキーボードアプリケーション/ソリューション（モバイルオペレーティングシステムに組み込まれている/プリインストールされているものなど）を使用する必要があります。

23. プッシュ通知に機密情報（機密またはそれ以上に分類されているシティ情報など）を含めることはできません。ただし、ワンタイムパスワード（OTP）はプッシュ通知で配布できます。
24. モバイルアプリケーションソリューションは、既知の/悪用可能な脆弱性のあるアプリケーションバージョンを使用するモバイルクライアントとの通信試行を拒否/無視する機能を備えている必要があります。
25. モバイルアプリケーションでは、[OWASP モバイルトップ 10](#) に記載されている回避対策を含むがこれに限定されない業界のベストプラクティスを遵守する必要があります。
26. 人工知能と機械学習（AI/ML）技術を活用するモバイルアプリケーションは、セクション 19 - **Error! Reference source not found.**（生成 AI/エージェント AI を含む）に従って、倫理的に行う必要があります。
27. モバイルアプリケーションは、シティが活用する目的/機能を実行するために必要な最小限のデバイス権限を活用する必要があります。
28. モバイルアプリケーションは、SD カードなどの外部/リムーバブルストレージに非公開情報を保存しないものとします。**Error! Reference source not found.****Error! Reference source not found.**

17.65 ソフトウェアに関する開示

サプライヤーは、シティに提供される製品またはサービスに含まれるオープンソースソフトウェアを含むがこれに限定されない、あらゆるソフトウェアコンポーネント（以下、総称して「ソフトウェアコンポーネント」という）を開示しなければなりません。サプライヤーは、更新、アップグレード、またはその他の方法で、シティのシステムにインストールされる製品またはサービスのバージョンにソフトウェアコンポーネントを導入しないものとします。ただし、各インスタンスにおいてシティに事前開示する必要はありません。さらに、サプライヤーは、その製品またはサービスには、契約においてシティが明示的に開示し承認していない義務に、シティまたはその関連会社を条件としてライセンスされるソフトウェアコンポーネントが含まれていないことを保証するものとします。サプライヤーは、発見後 30 日以内に、サプライヤーの組織、製品、またはサービス内で検出された悪意あるソフトウェアコンポーネントをシティに開示するものとします。具体的には、サプライヤーは、OWASP CycloneDX ファイル形式または ISO/IEC 5962:2021 ソフトウェアパッケージデータ交換（SPDX）仕

様ファイル形式において、製品またはサービスの各リリースおよびバージョンについて、シティに提供することにより、ソフトウェアコンポーネントの使用を開示するものとします。このような開示には、ソフトウェアコンポーネントの出所（商業ベンダー、埋め込みデータベース、ソースコードから構築された公開バイナリーパッケージマネージャー、埋め込みソフトウェア、キュレーションされたソフトウェアコンポーネントプロバイダーなど）、サプライヤーまたはそのソフトウェアサプライチェーン依存関係がソフトウェアコンポーネントのコピー（「フォーク」として知られている）を取得し、その後パッケージ依存関係として、または製品およびサービスがコンパイルされるサプライヤーのソースコードに組み込まれたソースコードとして製品またはサービスに組み込まれているかどうかを含める必要があります。

17.66 脅威モデリング

サプライヤーは、以下のすべてを包括的に取り扱う、および/またはこれらを網羅する脅威モデリングプロセスを実施しなければなりません。

1. 適用範囲の定義：サプライヤーは、脅威モデルの適用範囲を明確に定義し、シティの「機密」レベル以上の情報を処理、保存、または送信するソフトウェアコンポーネントおよびデータフローに焦点を当てなければなりません。
2. 脅威の特定：サプライヤーは、設計ライフサイクルの早い段階から、さまざまな攻撃ベクトルや脅威主体を考慮し、ソフトウェアの設計、アーキテクチャ、および意図された用途に関連する潜在的な脅威や脆弱性を体系的に特定しなければなりません。
3. リスク分析：サプライヤーは、特定された脅威を分析し、その潜在的な影響と発生の可能性を評価することで、セキュリティリスクの優先順位付けを行わなければなりません。
4. コントロール統合：サプライヤーは、優先順位付けされたこれらのリスクに対処するため、適切なセキュリティ対策およびリスク軽減戦略を策定し、ソフトウェアの設計および開発に組み込まなければなりません。
5. 文書化：サプライヤーは、特定された脅威、関連するリスク、および実施された対応策を含む脅威モデルを文書化しなければなりません。

6. 定期的なレビュー：サプライヤーは、特にソフトウェアの設計、機能、または導入環境に大幅な変更があった場合には、脅威モデルを定期的に見直し、更新しなければなりません。

17.67人工知能

1. サプライヤーは、シティに提供される、またはシティのシステムに統合されるすべての AI/ML システムおよびコンポーネントについて、堅牢なセキュアソフトウェア開発ライフサイクル（SSDLC）を導入し、これを遵守しなければなりません。これには、セキュアな設計、開発、テスト、導入、および継続的な保守が含まれます。
2. サプライヤーが提供する AI システムは、その運用において完全性を確保し、敵対的攻撃に対して強固な耐性を示さなければなりません。これには、不正なインジェクションの迅速な検出、入力のリネイズ、およびデータ分離の維持のための仕組みの導入が含まれます。
3. サプライヤーから提供される AI エージェントおよびコンポーネントは、シティのシステムやその他のツールと安全に連携できなければなりません。そのためには、強固な ID・アクセス管理、ツール実行引数の厳格な検証、およびリスクの高いツール操作の隔離が必要となります。繊細な操作やリスクの高い操作については、ヒューマン・イン・ザ・ループ（HITL）の仕組みを組み込む必要があります。
4. サプライヤーの AI システムは、すべての重要なイベントについて、包括的で改ざん不可能かつ監査可能なログを生成しなければなりません。これらのログは、シティのポリシーに従って改ざん、集計、保管から保護する必要があります。セキュリティ関連のインシデントや疑わしいアクティビティを特定し警告するには、継続的なモニタリングと異常検出機能が必要です。
5. サプライヤーの AI システムは、リスクベースの人間の監督をサポートし、適切な介入を可能にし、AI 出力と行動に明確な説明責任を持って設計する必要があります。これには、AI の出力をリスクレベルごとに分類することや、人間による上書き機能をサポートすることが含まれます。
6. サプライヤーが提供するすべての AI エージェント、コンポーネント、およびシステムは、堅牢な ID およびアクセス管理の統制措置を実装しなければなりません。AI とのあらゆるやり取りは、特定可能な識別子（人間または人間以外）に紐づけられる必要があります、すべてのアクセスには認証が必須

です。AI エージェントは、シティのリソースにアクセスする際、マネージド ID を使用し、最小権限の原則に従わなければなりません。

- a. サプライヤーは、シティのセキュリティポリシーの適用、一元的な ID 管理、および監査可能性を確保するため、すべての AI エージェントに Citi Object Identity Network (COIN) のエージェント ID を割り当て、シティの ID およびアクセス管理 (IAM) システムと連携させるよう手配し、これを確実に実施しなければなりません。
 - b. サプライヤーは、セキュアゲートウェイ (SSG Gateway や Apigee など) を通じて提供される COIN API を含む、シティが承認した統合メカニズムを用いて、サードパーティの代理店を COIN に登録しなければならず、また、シティの適用されるセキュリティ要件に従い、当該登録が安全な方法で行われるよう確保しなければなりません。
 - c. サプライヤーは、社内でホストされている場合、COIN に準拠したトークンを生成する必要があります。社外でホストされ、独自のフェデレーショントークンを使用してインバウンド認証を行うサプライヤーは、シティのトークンと交換可能なサポート対象のトークンを保有する必要があります (例: MSFT トークンから COIN トークンへの交換)。現在、取引所ではサポートされていない新しいトークンタイプについては、シティの IAM チームによる審査を経て承認を得る必要があります。
7. サプライヤーがモデルコンテキストプロトコル (MCP) のサーバーまたはクライアントを利用または提供する場合は、すべてのオプション機能を含め、MCP RFC 7591 を実装しなければなりません。
 8. サプライヤーの AI システムは、システムプロンプトと内部作業を開示または操作から保護する必要があります。コンテキスト管理では、テナント間、ユーザー間、または環境間のデータ漏洩を防ぐため、厳格な境界を設定する必要があります。
 9. サプライヤーは、敵対的攻撃、モデルの改ざん、AI による不正行為、または AI システムに関連するデータ漏洩など、AI 特有のセキュリティインシデントを検知、対応、報告するための手順を文書化してなければなりません。

。このようなインシデントについては、直ちにシティに報告しなければなりません。

18 安全な職場に関するガイドライン

適用対象：シティの情報へのアクセス/処理/管理/保管を行う、およびまたはインターネットに接続するシティブランドアプリケーションをホスティングする、およびまたはシティのネットワークリソースに接続する、およびまたはシティ施設に同伴者なしでアクセスする必要があるサプライヤー

サプライヤーはシティおよびそのクライアントの有形資産および無形資産を保護しなければなりません。シティおよびクライアントの資産は、承認された目的のために、承認された方法（適用されるライセンス、条件に従うなど）で、シティおよびシティのサプライヤーの事業目的に関してのみ使用することができます。資産には、現金、証券、物理的な資産、サービス、事業計画、シティの情報、サプライヤー情報、代理店情報、知的財産（コンピュータプログラム、モデルなど）および他のすべての個人情報、専有情報、機密情報が含まれます。シティ資産の不正な使用や許可されていない開示は、シティに対する義務違反となり、シティに対する詐欺行為となる可能性があります。同様に、シティの資産に関する不注意による、無駄な、または許可のない使用もシティに対する義務違反となります。

アイテム	要件
シティの情報（電子ドキュメントおよびハードコピーの書類）	通常の業務時間後、および、サプライヤーが指定されたワークスペースから離れる際は常に、シティの情報を、施錠された場所で安全に保管する必要があります。
デスクトップパソコン（PC）とノートパソコン	シティの情報へのアクセスまたは閲覧に使用する PC とノートパソコンは、一定時間操作されなければスクリーンセーバーのパスワードで保護する必要があります。サプライヤーは指定された作業エリアから離れる場合、CTRL + ALT + DEL を押して PC やノートパソコンをロックし、「コンピュータをロック」を選択する必要があります。サプライヤーがシティの情報を閲覧するためにノートパソコンを使用している場合、サプライヤーは、業務時間中、このようなノートパソコンがケーブルまた

アイテム	要件
	はセキュリティロックでベースユニットに固定され、通常の業務時間後はしっかりと施錠されていることを確認する必要があります。
施錠して保管	シティの情報を保管するファイルキャビネットや引き出しは、通常の業務時間後は施錠しておく必要があります。
開放されたオフィスエリア	開放されたオフィスエリアは、シティの情報を保管するファイルサーバー/ミニデータセンターとして使用しないでください。ただし、このような用途で設計され、シティとの間で文書化され報告されている場合は除きます。
プリンター、コピー機、ファックスのトレイ	シティに関連する資料はすべて、プリンター、コピー機、ファックスのトレイから取り除かなくてはなりません。
廃棄	不要になったシティの情報は処分してください（具体的な保管スケジュールに従ってください）。書類はシュレッダーにかけるか、安全な、または施錠されたリサイクル用ゴミ箱に入れてください。磁気メディアは適切な消去手順に従って安全に処分する必要があります。

19 人工知能/機械学習（生成 AI/エージェント型 AI を含む）

適用対象：提供する商品/サービスの一部に、シティが本サプライヤー要件において定義する、生成 AI/エージェント型 AI を含む人工知能/機械学習（AI/ML）を活用しているサプライヤー

19.1 サプライヤーは、契約に基づく該当するスケジュールまたは作業指示書で当事者間でこのような使用が合意されている場合を除き、以下に記載された AI/ML を使用しない業務委託先を確保しないものとします。

- a. シティと直接的または間接的に提供する契約を結んでいる商品またはサービス、あるいはその一部（そこに含まれるまたは組み込まれる第三者の商品またはサービスを含む）に使用、含有、またはその他の方法で組み込まれている、または
2. 当該 AI/ML がシティに提供される実際の商品またはサービスに使用され、含まれ、またはその他の方法で組み込まれているか否かにかかわらず、サプライヤーの契約の履行において何らかの方法で利用されている
3. シティの情報を AI/ML に公開する可能性のある方法でサプライヤーによって利用されている。これには、サプライヤーがその非商業的な事業活動（業務記録の保持、プロセスの改善、研究開発、コンプライアンス、内部監査など）において利用する AI/ML を含むが、これに限定されない。

19.2 サプライヤーがこれらの義務を遵守しなかった場合、本契約条件への重大な違反とみなされます。

19.3 規制当局から要求された場合、商品/サービスのいずれかの部分で AI/ML を使用することに関する規制当局の検査または法医学検査の一環として、サプライヤーは、AI/ML モデルを構成するアルゴリズムの実際の動作を発見するために必要なアルゴリズム監査の実施および/または実施を促進することを含め、規制当局の要請に応えるためにシティを支援しなければなりません。

19.4 また、以下の原則を遵守する必要があります。

合法性。 サプライヤー AI/ML は適用法を遵守するものとします。

目的と比例性。 サプライヤーは、コンテンツまたはシティの情報を、サプライヤーまたはサードパーティのデータと統合してはなりません。サプライヤーは、シティの書面による承認なしに、コンテンツまたはシティの情報をを使用して AI/ML をトレーニングしてはなりません。サプライヤー AI/ML は、本サービスの提供に必要な範囲を除き、コンテンツまたはシティの情報をを使用することはできません。

20 顧客からの苦情

20.1 苦情とは、口頭（対面または電話で）または書面（郵便または E メール、チャット、ソーシャルメディアなどの電子コミュニケーションを通じて）で受領されるもので、シティ、顧客ではない方、見込み顧客、シティのクライアント、見込みクライアント、またはクライアントの正式な代理人（以下総称して「顧客」）から、シティ、シティの従業員、シティの業務委託先、またはシティに代わって行動するサードパーティのサービスプロバイダー、または上記のあらゆる組み合わせによって提供されるシティのポリシー、商品またはサービスについて表明された不満をいいます。

20.2 サプライヤーは、シティの顧客苦情処理ポリシー、および適用されるシティの苦情関連の基準および手順を遵守するものとします。サプライヤーは、シティに代わってサプライヤーが提供するサービスに関連して、またはシティに関連する顧客（またはシティの「苦情」の定義に従い、非顧客もしくは見込み顧客）または規制当局からサプライヤーが書面または口頭で不満または懸念（それぞれ「苦情」）を受けた場合、24時間以内にシティの主要業務連絡先（または指名された者）に書面で通知するものとします。シティが当該システムをサプライヤーに提供しない限り、サプライヤーもまた、シティが合理的に満足するシステム（「追跡システム」）を開発、実施、維持して苦情を追跡し、独自の裁量でレポートのコピーまたはシステムへのアクセスをシティに提供します。追跡システムは次のことを行います。

- a. 苦情を種類、受領日、および苦情の通知がシティに提供された日付で分類します。
- b. 苦情が解決されるまで、その処理の経過を追跡します。
- c. その他、シティが合理的に要求する事項のすべてを提供します。追跡システムは、サプライヤーが（シティと協議の上）サプライヤーの事業または本サービスの提供に関して体系的な問題があるかどうかを判断し、問題を速やかに是正できるように、特定の事項に関して異常な数の苦情を受け取ったかどうかを判断できるよう設計される必要があります。

21 個人での売買および投資に関するポリシー

シティの個人での売買および投資に関するポリシー（PTIP）は、対象者のブローカー口座または取引口座の維持、開示、監視に関する許可された禁止された取引および投資活動、事前承認要件、および要件を定義するものです。シティまたは第三者に関する(1)重要な未公開情報または内部情報（以下総称して「MNPI」）に関する個人の知識、または(2)顧客の証券、デリバティブ、コモディティのポジション、取引および戦略に関する情報など、個人の地位またはシティとの関係が不適切に利用されることを防止するため、法令遵守を促進するための最低限の基準を定めるものです。

シティでの職務の一環として MNPI に定期的にアクセスする必要がある、対象者および/またはシティアクセス担当者に指定されるサプライヤー従業員は、PTIP 内の要件を遵守する必要があります。 サプライヤー従業員は、個人口座の開示、個人取引アクティビティの事前承認、および個人取引の制限、および定期的な取引明細書の提出に関する ICRM からの要求を遵守する必要があります。

22 請求と請求書作成基準

サービスの適時性を改善し、管理を強化するためのシティの取り組みに関連して、すべてのサプライヤーは、以下に詳述されるように、シティの請求書提出に関する優先方法、および優先される請求書支払い方法をサポートするものとします。

- サプライヤーは、シティがサプライヤーに通知した形式でシティに送信される電子ファイルを作成し、シティの iSupplier ツールを活用して、シティへのデジタル送信に必要な請求書/請求データを入力します。
- サプライヤーは、サプライヤーへの電子決済を促進し、シティが提供するバーチャルカード決済を利用するために、必要なすべての銀行情報および裏付けとなる文書をシティに提供します（利用可能な場合）。

注：支払条件は、シティが請求書を受領した日を起算日とします。

シティは適時に支払い、契約上の約束を満たすために、すべてのサプライヤーに以下の請求書データを含めることを義務付け、商品またはサービスのシティへの請求時に関連するガイドラインを遵守することを求めます。

1. 正しいシティの事業体、「請求書送付先」の住所、および関連するシティの事業担当者名
2. 請求書番号、請求書日付、発注書番号
3. 請求書は、シティの発注書に記載されたシティの所在地または E メールアドレスに送信すること
4. 請求される商品またはサービスには、請求書内に明確で説明的な詳細が記載されている必要があります。
5. 特定の請求書に対する現在の請求額のみを含めてください（保留中の他の請求書の未払い残高は含めないでください）。
6. 請求書は、裏付けとなる書類を含め、英語による記載としてください。

23 職場離脱ポリシー

シティの職場離脱は、機密性の高い活動またはリスクの高い活動、特に会社の帳簿や記録に影響を及ぼす活動を行う個人が、これらの義務を定期的に回避するよう義務付けられています。この強制的な分離は、そうでなければ見過ごされてしまう可能性のある不正、窃盗、その他の不正行為を発見する機会を創出することで、内部統制を強化することを目的としています。このポリシーは、機密性の高い職務に就いている人員に必要な欠勤について、米国連邦準備制度理事会が定める監督上の期待と一致するものです。

シティにおいて、職務の一環として機密データへのアクセス権限を持ち、**かつ**「機密取扱者」に指定されているすべてのサプライヤー従業員は、**MA** ポリシーの要件を遵守しなければなりません。該当する従業員は、毎年、すべてのポリシーや規則・制限に従い、義務的な欠勤期間を設定し、その期間を完全に消化する必要があります。この期間中、彼らは機密性の高い活動を行ったり、指示・許可・承認を行ったりしてはならず、また、保険適用に関する問い合わせを転送する場合を除き、顧客とのやり取り

を含むいかなる連絡に対しても実質的な回答を行ってはありません。欠勤期間が開始後に中断する必要がある場合、システムへのアクセス権限を回復させるためには、マネージャーまたはシティの担当者がコンプライアンスシステム上でその欠勤期間をキャンセルする必要があります。その後、従業員は新たな欠勤期間を再設定する必要があります。

付録 - 定義

エアギャップとは、コンピュータ、システム、またはネットワークを他のコンピュータ、システム、またはネットワークから物理的に隔離するセキュリティ対策です。エアギャップで隔離されたデータバックアップ構造により、サイバー攻撃への曝露を制限し、攻撃が始まる前の時点でデータを復旧することが可能になります。

適用法には、(a)州の競売法および規制、並びに(b)2003 年公正かつ正確な信用取引法のセクション 114 を実施する通貨監督庁を含む米国連邦機関が発行する各種規則、ガイドラインおよびその他のリリース（レッドフラッグガイドラインおよび規制と呼ばれることもあります）が含まれています。

アベイラビリティゾーンとは、クラウドサービスプロバイダーが論理的なデータセンターのグループを持つ場所です。アベイラビリティゾーンは、クラウドリージョン内にある、電力、ネットワーク、通信を冗長化した 1 つまたは複数の個別のデータセンターのことです。

人工知能（AI）とは、コンピュータプログラムを介して人間の知能を模倣し、従来の統計学、数学、計量経済学、金融学的アプローチを超える方法で推定、予測、推奨、決定を行う定量的手法、システム、アプローチ（「技術」）を指します。これには、以下に示すすべての AI カテゴリーと、AI のあらゆるバリエーションが含まれます。例えば、生成 AI、エージェント型 AI、大規模言語モデル、汎用 AI（GPAI）モデルなどです。

AI カテゴリーは以下の通りです。

- o **静的 AI**：オフラインで手動でトレーニングされた、またはパラメーターが明示的にプログラムされた、推定、予測、推奨、または決定を行うために使用される AI 技術
- o **動的 AI**：「静的 AI」とは異なり、実稼働環境で定期的にパラメーターを自動的に再トレーニングできる技術
- o **自動 AI**：基本構造（ハイパーパラメータや入力変数など）を自動的に変化させることができる「動的 AI」技術
- o **認知 AI**：特別な訓練を受けていない事項についても、自律的に判断し行動することができる技術

機械学習(ML)は、AI のサブセットであり、ランダムフォレスト、ニューラルネットワークベースのアプローチなど、すべてのパラメーター表現やコンピュータのステップを明示的にプログラミングすることなく、データから表現や推論を導き出します。対照的に、ML のサブセットに

は含まれない AI 技術には、ファジーロジック、自然言語処理のための複雑な依存関係解析技術などの技術が含まれます。

ビジネス活動担当責任者（BAO）は、サプライヤーとの関係に基づく特定の活動の遂行および積極的な管理に責任を負うシティの従業員です。

ビジネスイントロデューサーとは、シティが採用するサプライヤーで、新しいビジネス機会を発掘したり、既存の顧客関係を管理したりするためにシティに代わって行動します。

ビジネス上の贈答品は、シティのビジネスまたは外部当事者のビジネスに関連してシティの従業員が授受する、価値のある物品（ビジネス接待以外）です。通常、25 米ドル以下の物品は除きます。

シティの情報は、保管、処理、送信、または廃棄中にデジタルおよび非デジタル両方の形式で、シティが所有する、またはシティが保護する義務がある情報です。

シティ情報分類には以下が含まれます。

機密情報とは、シティの事業部門および/または関連当事者に関する情報のことで、個人を特定するものではなく、高度な保護を必要とする情報です。この情報の機密性、整合性、または可用性が損なわれると、シティの業務、財務状況、フランチャイズ、または法人クライアントに重大な影響を及ぼす可能性があります。

個人を特定できる機密情報とは、個人に関する個人情報であり、当該個人に対するなりすまし、信用詐欺、その他の金融詐欺などの違法行為を助長する可能性があるものです。この情報の機密性、整合性、または可用性が損なわれると、金銭的損失または不正行為を含むがこれに限定されない、個人に大きな影響を及ぼす可能性があります。

o 他の個人情報と組み合わせることで「機密」に分類される個人データ要素には、以下の情報と組み合わせた個人名および連絡先情報（住所、電話番号、またはメールアドレス）が含まれます。

- 資金移動につながる可能性のある、または以下のようななりすまし犯罪や詐欺行為に利用される可能性のある取引データ要素
- クレジットカード番号/デビットカード番号
- カードのセキュリティーコード（CVV）またはPIN
- クレジットレポートデータ（クレジットスコア）
- 生年月日
- 従業員のパフォーマンス（評価/フィードバック）、または報酬情報

- CCTVやATMの記録を含むビデオ録画記録
- 以下のような、単独で機密 PII を構成できる特定の個人データ要素
 - 米国の社会保障番号または政府発行のID番号（米国社会保障番号と同等の用途および/または法的保護を提供するもの）、パスポート番号、運転免許証番号、個人納税者番号

社内情報とは、個人に関する情報ではなく、ビジネス目的のための情報であり、中程度の保護が必要です。この情報の機密性、整合性、または可用性が損なわれると、チームまたはワークグループに**限定的な影響**が及ぶ可能性があります。

- **個人を特定できる情報（PII）** 個人情報とは、以下のいずれかの情報を意味します。
 - 個人または世帯（名前、署名、住所、社会保障番号や住民登録番号などの固有の国民識別番号、生年月日、運転免許証番号など）の身元を特定する情報、または個人の身元を特定する、または特定するために利用できる情報
 - 個人または世帯に関連する、それを説明する、それと関連付けが可能な、またはそれに妥当にリンクできる（直接または間接的に問わず）情報
 - 個人の認証またはアカウントへのアクセスの提供に利用できる情報
 - （ユーザー名、メールアドレス、パスワード、PIN、ID 番号、セキュリティ質問への回答など）または個人に関連するもので、機密性の高い可能性がある情報（個人の医療情報や健康情報、口座番号、口座金額など）
 - 個人情報にはまた、保護の対象となる健康情報（米医療保険の相互運用性と説明責任に関する法律により定義）、機密個人情報およびクレジット情報（様々なデータ保護 / プライバシーおよび銀行守秘義務法により定義）が含まれます。

公開情報とは、シティのプレスリリースやシティに関するニュース記事など、社外の人々が自由に入手できる情報、または一般社会での使用が意図されている情報です。

制限付き情報とは、シティまたはその関連会社にとって最も機密性が高く、最高レベルの保護を必要とする特定の人物またはグループによって使用が制限される情報です。この情報の機密性、整合性、または可用性が損なわれると、シティの業務、財務状況、フランチャイズ、または法人クライアントに**重大（全社的、複数の地域、複数の部門）の影響**を及ぼす可能性があります。

- **機密 PII** とは、特定の法律により追加的な保護が必要とされる個人情報で、不当に差別化したり、不当に不公正になったり、個人に損害を与えたりする可能性があります。この情報の機密性、整合性、または可用性が損なわ

れると、金銭的損失または不正行為、差別的影響を含むがこれに限定されない、個人に大きな影響を及ぼす可能性があります。

- 特に、次に関連するデータ：人種、宗教、信仰または哲学的信条、民族性、所属する政党または政治的意見、組合への加入有無、犯罪歴または刑法犯罪、遺伝子データ、生体データ、または個人の性的指向または活動に関するデータ。

- 個人の病歴や精神的・身体的状態に関する情報を含む個人の健康情報(PHI)。

クライアントとはすべてのシティのクライアントまたは顧客を指し、個人（自然人など）、事業体、機関、組織、法人が含まれる場合があります。

クラウドリージョンは、クラウドサービスプロバイダーがデータセンターをクラスター化している物理的な場所です。

通信機器、システム、およびサービスとは、文字、音声、動画による電子コミュニケーションに使用されるハードウェア、ソフトウェア、またはアプリケーションです。電子コミュニケーションチャンネルには、コンピュータ、ノートパソコン、タブレット、「Bring Your Own Device」(BYOD)を含むモバイル機器または携帯電話、BlackBerry、電話機、ファクシミリ（ファクスサービス）、イントラネットおよびインターネットアクセス、Wi-Fi サービス、Eメールサービス、Microsoft Lync、Skype、Bloomberg メッセージなどのインスタントメッセージサービス、コミュニケーション機能が埋め込まれたウェブサイトおよびアプリケーション、Zoom や Microsoft Teams などのビデオ会議またはコラボレーションプラットフォーム、ソーシャルメディアサービス、インタラクティブな情報共有サービス、第三者チャットルーム、電子掲示板、およびブログが含まれますが、これに限定されません。

コンテンツとは、シティの機密情報、およびその他のあらゆる種類のデータ、レポート、統計、または情報で、(a)シティもしくはその関連会社、またはその顧客、顧客もしくはサービスプロバイダーにより、またはそれらの代理として、サプライヤーに直接または間接的に提供または利用可能となったもの、(b)本サービスを通じて作成、生成されたもの、または(c)上記のいずれかから派生したもの、を指します。

契約とは、2 人あるいはそれ以上の当事者によって署名された書面による法的文書で、両当事者の提示、承諾、約因、義務および目的の合法性が記載されています。契約の例として、商品およびサービスに関する基本契約書、作業明細書/作業指示書、修正と補遺、付属書類、発注書、その他、シティの事業体およびサプライヤーが署名した書面によるあらゆる文書が挙げられます。秘密保持契約（NDA）も、本基準の目的上、契約とみなされます。

アクセス拒否（DOA）テストは、定義された RTO 内に復旧可能なシティのビジネスプロセスのためのサプライヤーの人材配置とサポートを検証します。

サービス拒否（DOS）テストは、シティのビジネスをサポートするサプライヤーのアプリケーションおよび基盤となるインフラストラクチャ構成要素が、定義された RTO 内に復旧可能であることを検証するものです。

「**預託資料**」とは、以下のサブセクション(i)～(vi)を総称して指します。これは該当する場合、シティ環境内での業務のためにシティにライセンスされているソフトウェアまたはシティに提供されるホスティングサービスのためにサプライヤーが使用する資料を意味します。

- (i) シティとの該当する契約に定められた使用許諾されたソフトウェアまたはホスティングサービスの開発、運用、メンテナンス、サポートに使用されるソフトウェア用のソースコードの正確な重複バージョン（および当該ソフトウェアまたはホスティングサービスのすべてのその後のバージョン）、および当該ソフトウェアのすべての文書（シティにすでに当該ソースコードの一部のコピーがあるかどうかに関係なく）（以下「**ソースコードデポジット**」）
- (ii) サプライヤーがライセンスを受けたソフトウェアまたはホスティングサービスの開発、運用、メンテナンスおよびサポートに関して権利を有する第三者ソフトウェアへのソースコード
- (iii) ソフトウェアまたはホスティングサービスを運用、メンテナンスおよびサポートするために必要な、預託資料に含まれるソースコードを実行可能な形式に変換するために必要なデバッガー、アセンブラ、コンパイラなどのすべてのソフトウェアツールのライセンスコピー
- (iv) 上記で規定されていない限りにおいて、以下を規定する文書：**(A)**預託資料の一般的な説明と操作、**(B)**アーキテクチャと基本的なプログラム機能、**(C)**データフロー情報、**(D)**詳細なメモリマップとリスト、**(E)**入出力ポートマップ、**(F)**該当するプログラミング言語の通常の知識を有するプログラマーが預託資料に含まれるソースコードを使用および変更することを可能にするその他の詳細
- (v) シティまたはシティに代わって権限を有するサードパーティがソフトウェアまたはホスティングサービスの使用、運用、変更および強化できるように合理的に求められる、本ソフトウェアまたはホスティングサービスに関連するその他のすべての技術情報
- (vi) ソフトウェアまたはホスティングサービスに関連して使用されるすべてのサードパーティのソフトウェアおよびテクノロジーのリスト。これには、ソフトウェアでの使用に関する合理的な詳細および当該ソフトウェアまたはテクノロジーのプロバイダーの

ための連絡先情報が含まれます。シティは、第(ii)項に定める場合を除き、預託資料に第三者のソースコードが含まれていないことを認め、これに同意するものとします。

(vii) ホスティングサービスに関して

- a. クラウドホスティングされた実稼働環境または環境固有のクラウド関連資料およびシティの実稼働環境を再現するために必要なその他の情報のスケールダウンレプリカ（ただしこれに限定されない）：コードとしてのインフラストラクチャ、テラフォーム・スクリプト、クラウド・リソース、クラウド形成テンプレート、構成ファイル、クラウド・テナント、クラウド・サブスクリプション、マシン・イメージ、ドッカー・イメージ、および本ソフトウェアのソースコードとしてのインフラストラクチャ
- b. 本ソフトウェア内に保持されているシティのデータのコピー

電子コミュニケーションとは、有線または無線信号で電子的な手段によって人員により送信、受信、または使用されるメッセージまたは情報です。電子コミュニケーションには、テキストメッセージ、Eメール、P2Pメッセージ、インスタントメッセージ、ブログの記事、ソーシャルメディアの投稿、WhatsApp、WeChat、LINE、Signal、Viberなどのメッセージアプリケーションを通じて送信されたメッセージ（添付ファイル、スクリーンショット、録音・録画された音声や動画ファイル、ライブの音声ファイルや動画ファイルを含む）、および電子コミュニケーション機器、システム、およびサービスを介して作成、受信、ダウンロード、保存、送信、削除、または使用されたファイルが含まれますが、これらに限定されません。

職務IDはADMINやROOTなどの一般的なIDで、セキュリティシステムにアクセスする担当者またはプロセスによって使用されます。IDおよびアクセス管理（IAM）における主要なイニシアチブは、職務IDの使用に伴うリスク防止のために、シティが具体的かつ明確な管理体制を完備していることです。

フランチャイズ基幹業務プロセス/フランチャイズ基幹業務用アプリケーション（FCA）は、フランチャイズ基幹業務機能を正常に遂行するために重要なものとして、シティにより特定されたプロセス/アプリケーションです。

不正とは、他人を欺くことを目的とした意図的な行為、虚偽の陳述、または不作為であり、その結果、被害者は損失を被り、または加害者は利益を得ます。

ホスティングサービスには、インストールされたアプリケーション、およびホスティングサービスを提供するためにサプライヤーが管理または利用する施設および環境、ホスティングサービス環境内にインストールまたは使用されるすべてのアプリケーションおよびその他のソフトウェア、データベース、ウェブサイト、サーバー、ハードウェア、ネットワーク、電気通信お

およびその他の機器、およびその他の技術、およびいずれの場合も、すべてのアップデートおよびサポートサービスも含まれますが、すべてのコンテンツおよびシティのシステムは含まれません。

本人確認データ (IVD) は、セキュリティに関する質問 (SQ) または知識ベース認証 (KBA) の質問として定義されます。セキュリティに関する質問は通常、アプリケーションによって定義され、エンドユーザーによって回答されます。母親の旧姓、出生地、好きなアイスクリームなどが例として挙げられます。どちらのタイプの質問も、認証データとして扱う必要があります。

情報セキュリティ (IS) とは、コンピュータまたはコンピュータが不正アクセスや攻撃から保護されている状態を指します。そして、この状態が保たれているため、**(a)** コンピュータまたはコンピュータシステムを継続的に利用および操作することができ、**(b)** コンピュータまたはコンピュータシステムの整合性が維持され、**(c)** コンピュータまたはコンピュータシステムに保存、処理、または送信されるデータの整合性と機密性を維持することができます。

IS の脅威 とは、攻撃を受けたコンピュータまたはコンピュータシステムに保存された IS、または他のコンピュータやコンピュータシステムを危険にさらしたり悪影響を及ぼしたりしかねない（既知のまたは疑わしい）行動または活動を意味します。

IS の脆弱性 とは、単一または複数の IS の脅威に利用され得る、コンピュータまたはコンピュータシステムの弱点や欠陥等を意味します。

非クライアント/非収益創出 は、法的活動、監督業務、規制活動、ビジネス継続性活動を含む、収益創出活動に関連しないビジネスクリティカルな活動として定義されています。

秘密保持契約 (NDA) は、シティとサプライヤーの間に締結される契約であり、情報の交換、使用、開示は当該契約の条件によって管理されます。

オープンソースソフトウェア とは、ソースコードまたはコンパイルされたコンピュータプログラムであり、そのソースコードが一般公衆に利用可能であり、元の設計から変更することができるものを指します。

人員 とは、直接記載されているか文脈から導かれるかにかかわらず、サプライヤーおよびその関連会社、取締役、役員、従業員、代理人、監査人、コンサルタント、サービスプロバイダー、および業務委託先（シティ従業員を除く）を指します。サプライヤー人員には、業務委託先の取締役、役員、従業員、代理人、監査人、コンサルタントまたはその他代表者も含まれます。

記録インベントリとは、記録の種類、保管場所、日付などを含むシティの記録の詳細な一覧で、情報のライフサイクル全体を通じて記録を適切に管理する上で業務に必要なものを指します。

情報保留は、記録・情報に対して課される要件で、保留を要請した当局によって解除されるまで、変更または処分が保留されます。

復旧能力とは、サプライヤーの製品・サービスの提供の容量、数量、速度を通常の製品・サービス提供の割合で示したものです。

復旧期間とは、サプライヤーが復旧モードで業務を継続できる最長期間を暦日で示したものです。

目標復旧時点とは、ビジネス中断後にデータを復旧する必要がある過去の時点のことで、時間単位で示されます。これは、重大インシデントによって IT サービスからデータが失われる可能性のある最大目標期間です。**RPO** は、IT サービスに影響を及ぼす重大インシデントが発生した場合にデータが失われる可能性のある最大期間の目安にすぎません。例えば、前日の処理の終了時までに、どの程度のデータが失われる可能性があるかを直接測定するものではありません。

目標復旧時間とは、サービスの中断から製品・サービスの復旧までの時間を指します。

「公表事由」とは、以下のいずれか 1 つ以上を意味します。

- (i) サプライヤーが、(A)債務を支払うことが不能となり、または債務を支払うことができない状態に陥った場合、(B)国内または外国の破産法または倒産法に基づく手続に、自発的または非自発的に、7 営業日以内に完全に停止されない場合、または申立てから 45 日以内に却下または取り消されない場合、(C)債権者の利益のために一般的な譲渡を行った場合、(D)管轄権を有する裁判所により命じられた受任者、信託管理人、保管者、または類似の代理人を任命され、その財産または事業の重要な部分を管理または売却する権限を有している場合。

リソース管理組織 (RMO) は、シティのためにエンドツーエンドのグローバルリソースを管理する責任を負います。これには、戦略的ソーシング、購買から支払いまでの業務、人材配属オフィス、およびサプライヤー管理フレームワークが含まれます。

RMO ソーシングマネージャーは、リソース管理組織(RMO)内の個人で、提案依頼書や他のサプライヤーの選定、契約条件の管理、財務評価認定要件を含む、契約ビジネス条件、要件、価格の交渉に対する責任を担います。

個人に対する**重大または致命的な悪影響**とは、個人が相当な悪影響を受ける可能性が合理的に見込まれるもので、これには金銭的損失、解雇、再就職が不可能または困難な状況、人権の喪失、個人的屈辱または公での侮辱、または不当な拘禁が含まれます。

業務委託先：業務委託先とは、シティが第三者に委託契約しているサービスまたは活動の一部またはすべてを遂行するために第三者が採用した第四の当事者（個人または事業体）を指します。

ガイダンス

質問 1: サードパーティの業務委託先をすべて報告する必要がありますか？

回答 1: 報告する必要があるのは、実施されるサービスに関連する業務委託先のみです。業務委託先が行うサービスや活動の例として、以下のものが挙げられますが、これらに限定されるものではありません。

- * シティが第三者と契約したサービス/活動を直接的または間接的にサポートするテクノロジーまたはソフトウェアサービスを行う業務委託先
- * シティの機密またはそれ以上の情報へのアクセスがサービスに含まれる業務委託先
- * 既存のまたは潜在的なシティのクライアントと直接的または間接的にやり取りする業務委託先
- * シティ施設内または施設外で、付き添いなしでシティの文書のシュレッダー処理またはアーカイブサービスを行う業務委託先
- * 支払い、回収、貸付など銀行業務の中核となる機能やサービスをサポートする業務委託先

サプライヤー：この「シティサプライヤー要件」文書の目的上、「サプライヤー」とは、シティ事業体に直接製品またはサービスを提供するために、またはシティ事業体のビジネス目標を達成するためにシティ事業体をサポートするためのビジネス上の取り決めを締結した外部の第三者のみを指します。外部の第三者は、シティ以外の事業体を指します。サプライヤーはまた、シティ事業体のクライアントまたは顧客であることもあれば、シティのクライアントおよび顧客とのやり取りをサポートする場合もあります。ただし、シティのクライアントまたは顧客であることのみに基づく取り決めは、本書の適用範囲内において、サプライヤーとの関係とはみなされません。

一時的情報：記録とは、法律上、規制上、または承認された業務上の理由でシティが保持する義務がある、最終的かつ完全な状態の情報です。その他のすべての情報は、一時的情報に分類されます。